TYÖ- JA ELINKEINOMINISTERIÖ
ARBETS- OCH NÄRINGSMINISTERIET
MINISTRY OF EMPLOYMENT AND THE ECONOMY

Data protection in working life

Data protection in working life

Introduction

An employer's activity involves a need to collect personal data on employees. Protection of privacy, on the other hand, entails the greatest possible right of a job applicant, employee and *civil servant* to know and decide about the *processing* and content of his or her own personal data and the right to be assessed on the basis of correct personal data. That is why it is important for the parties to working life to know how matters relating to the processing of personal data are resolved specifically at workplaces.

The Act on Protection of Privacy in Working Life (759/2004), subsequently *The Act on Data Protection in Working Life* will enter into force on 1st October 2004. The Act supplements the former Act on Protection of Privacy in Working Life (477/2001). In the new Act, the provisions of the former Act are the earlier ones as to their content, but the structure of the Act has changed. The Act incorporates provisions on drug tests, camera surveillance and the protection of e-mail.

The Personal Data Act (523/1999) and the Act on the Protection of Privacy in Electronic Communications (516/2004) incorporates general provisions relating to data protection which are also applied in working life beside this special Act.

This brochure seeks to provide an overall picture of data protection in working life.

General provisions (§ 1- § 2)

The purpose and scope of application of the Act

The purpose of the Act on Data Protection in Working Life is to respond to questions concerning the protection of private life specifically in the area of working life. It relates solely to the relationship between employee and employer.

The Act applies to *employment relationships.* The scope of application covers all employment relationships regardless of whether they are based on the Employment Contracts Act, the Seamen's Act, the Act on the Employment Relationship of a Household Employee or whether they are relationships based on an apprenticeship contract.

The Act applies to *civil service relationships and to comparable service relationships.* The Act relates to state, municipal and church officials or to people in the service of independent public institutions. At the same time, civil servants are also affected by certain special provisions, including the Act on the Publicity of the Activity of the Authorities, the Register Act, the Act on State Officials, the Church Act etc.

Where applicable, the Act also applies to *job applicants and people applying for civil service relationship.*

General conditions for processing personal data (§ 3- § 5 a)

Necessity requirement

An employer may process only personal data that are directly necessary as regards an employee's employment relationship, relating to the management of the rights and obligations of the parties to the employment relationship or the *benefits* provided to employees by the employer or which are due to the *special nature of the work*. No exception may be made to the data having to be necessary even with the employee's consent, and this requirement of necessity shall be implemented alongside the other more detailed provisions of the Act.

In connection with the planning of data *collecting* already, an employer must define the necessity for examining the data in such a way that it is evident for which kinds of tasks the personal data are to be *collected*. This kind of assessment must always be performed in each case separately.

For practical reasons, it is impossible to list all of the personal data which an employer is entitled to *process.* Situations in working life vary according to sector or task. An employer requires an employee's personal data for a variety of reasons such as for the authorities when dealing with taxation and social security payments, for the management of the personnel administration and development of the organisation, for customers etc. As regards personal data concerning the *collecting* of which some other act lays down separately, an employer no longer needs to consider the necessity of *collecting* the data.

Data that are necessary as regards managing an employer's and employee's rights and obligations include, for example, data relating to the performance of tasks, selection of an employee, working conditions and compliance with the regulations in collective agreements. Data relating to the *benefits* provided by an employer can relate, for example, to swimming pool tickets and discounts provided by an employer and to the use of these. Data based on *the special nature of work* can relate, inter alia, to the family circumstances of an employee who is to be transferred to assignments abroad whenever the employer is responsible for the education of the children.

In recruitment situations, an employer has to assess the necessity for data with regard to the job which the person has applied for. This mainly means data showing the applicant's competence and suitability and also a statement on the job applicant concerning his or her suitability health-wise for the job.

For a violation relating to the *processing of* personal data contrary to the Act on Data Protection in Working Life, an employer or its representative is sentenced on the same penal scale and for the same offence as for corresponding violations of the Personal Data Act, i.e., for *a personal data offence* (Chapter 38, § 9, of the Penal Code), to either a fine or imprisonment for a maximum of one year. The act should violate the protection of the employee's privacy or cause the employee other damage or fundamental inconvenience. The act requires intent or gross negligence when processing the personal data of the employee in a manner contrary to their purpose or when violating the necessity requirement of the data.

Destruction of unnecessary information

Outdated or unnecessary data must not be kept. The provisions of the Personal Data Act on this matter are also applied in working life. Such provisions include § 9(2), § 29, § 34 and § 35, and § 48(2).

The legislation contains special provisions on the retention periods for personal data which an employer must comply with. These provisions include, for example, the periods of limitation according to the Contracts of Employment Act, Working Hours Act and the Bookkeeping Act. In public administration there are also special regulations on the retention of personal data on employees and officials.

Ban on discrimination

The *collecting* of unnecessary data may lead to discrimination, and so the bans on discrimination in the legislation are of significance to the *processing* of personal data, starting from an assessment of their necessity. Provisions relating to the ban on discrimination are to be found in the Constitution, Employment Contracts Act, Non-Discrimination Act, Act on State Officials, Act on the Service Relationship Security of a Municipal Office Holder, Church Act, Act on Equality between Men and Women and in the Penal Code.

General preconditions for collecting personal data of employees and the employer's obligation to notify

Personal data refer to all kinds of records describing the characteristics or living conditions of an employee. Personal information can be information that is written or recorded mechanically, electronically, optically or magnetically but not solely oral information unless it is based on information recorded in *a personal data file*.

Processing of personal data refers to the *collection*, recording, organising, use, transfer, surrender, retention, alteration, combining, protection, deletion and destruction of personal data and to other measures affecting personal data.

Personal data register refers to a file that is kept manually or by means of automatic data-processing. The employer is the controller. The delegation of the management of employment relationships to an outside body does not remove the position of controller or obligations from an employer. Nevertheless, it has to be observed that an implementer of occupational health services has an independent position as a keeper of a personal data file that does not depend on an employer. For this reason, a *personal data file of an occupational health person and an employer's personal data file must not form an entity.*

An employer must primarily *collect* personal data from the employee personally because, in that way, the employee is best able to determine what data are being *collected* about him or her. If an employer *collects* data from elsewhere, he or she must obtain the employee's consent for this. Consent is not required whenever an authority passes on information to an employer for carrying out a duty that is laid down for the latter in law or whenever an employer obtains personal credit data or criminal record data in order to ascertain an employee's trustworthiness. In those cases, too, it is required that the personal data obtained are necessary as regards the employment relationship.

For example, data supplied to an employer by a distraining authority for the purpose of distraining pay are data of this kind.

An employee's credit data can be necessary in jobs where the person will have direct financial responsibility for the employer's assets or whenever the employment relationship otherwise calls for particular trust. The Personal Data Act (§ 20 (4)) lays down concerning when personal credit data may be passed on and the fact that an employer must also notify a job applicant of the acquisition of credit data if their use will affect decision-making (§ 25(2)). On the other hand, the Criminal Record Act and Decree lay down concerning the purposes for which criminal record data can be surrendered and to whom.

At some workplaces, particular information is required on the trustworthiness of personnel. These workplaces can include airports, nuclear power stations, telecommunications operator centres, certain ADP service companies, production plants and research institutions, and the authorities. For these jobs, the Act on Safety Clarifications is applied. The Act includes provisions on the grounds for these clarifications.

If an employer obtains information in order to determine the trustworthiness of an employee, the employer should, prior to obtaining the information, tell the employee of its intention to obtain such information. This obligation to notify relates not only to personal credit data and criminal record data but also to other data obtained in order to ascertain trustworthiness which an employer *collects* on the basis of an employee's consent elsewhere than from the employee personally. An employer must notify an employee personally of data that are *collected* elsewhere than from the employee personally, and of their content, before the data are used in decision-making affecting the employee. The employer is obliged to inform the employee on his own initiative.

An employer or its representative who violates the aforesaid obligation to notify, deliberately or through gross negligence, can be sentenced to a fine for violation of the Act on Data Protection in Working Life.

An employer's obligation to notify and an employee's right to check data on him- or herself are also governed by what is laid down thereon elsewhere in law. Unless otherwise provided elsewhere in the Act, at least § 24, § 26 - § 28 of the Personal Data Act, as well as s 12 - § 16 of the Act on the Publicity of the Activities of Authorities will be applicable.

The co-operation legislation (Act on Cooperation within undertakings and Act on Cooperation in State Departments and Agencies) includes provisions on the basis of which data collected during an employment relationship as well as at the start of the employment relationship fall within the scope of the cooperation procedure. An employer should negotiate with personnel representatives when deciding about the introduction of new personal data systems and their content as well as about other data to be collected, including information obtained by means of a variety of tests. Nor does the cooperation procedure allow agreement on the collecting of data which do not meet the requirement of necessity contained in law.

Processing health information

Health information is sensitive information, and so an employer's right to process data on an employee's health has been particularly restricted in law.

An employer may process an employee's health information solely if the employee personally supplies him or her with them or if the employee has given written consent for such information to be passed on to the employer. Whenever an employee personally passes on information relating to his or her health, this meets the characteristics of consent. Nevertheless, an employer may not process, even with the employee's consent, any information on health.

The Employment Contracts Act and collective agreements contain regulations on salary payment during sick leave. In the agreement regulations, the periods during which salary is to be paid in the case of sick leave are clearly longer than those in the Act and they are applied quite comprehensively not only with regard to employers who belong to unions but also, on the basis of the general binding nature of the collective agreements, to companies that do not belong to employer unions. As a rule, in the agreements, the precondition for payment of salary during sick leave is that the employee must supply the employer with a doctor's certificate, in particular whenever illness has lasted for more than three days. In addition, almost all of the agreements contain a regulation according to which an employer is to apply for reimbursement according to the Sickness Insurance Act for the period in which he or she pays salary to the employee. A doctor's certificate must be attached to the application. Sick leave pay is not usually paid if the employee has caused incapacity for work deliberately or through gross negligence. On the other hand, if an employee has several sick leaves in succession, the length of the payment period may be affected by whether a relapse of the same illness or a different illness is involved. The agreements also contain regulations on the basis of which an employee can be entitled to remuneration for the duration of a specific intervention or examination even though he or she might not be exactly incapable of work. The aforesaid agreements have been construed to mean that an employer is entitled to find out the details of the medical diagnosis on the basis of which the employer examines whether the employee is entitled to sick leave pay.

The aforesaid practice can continue because an employer is entitled to process information on an employee's health which contain information on the diagnosis if it is necessary

- for the payment of sick leave pay or comparable health-related benefits (e.g., a visit to a doctor, during which is agreed that salary will be paid, for the purposes of examinations or treatment without the employee being incapable of work) or
- in order to determine whether there is a justified reason for absence from work.

Nevertheless, an employer's right to process an employee's detailed health information does not mean that the employee is under an obligation to supply the employer with a doctor's certificate containing details of the diagnosis. If the employee fails to supply a certificate of this kind, he or she may forfeit sick leave pay. In these cases, he or she may apply personally for reimbursement according to the Sickness Insurance Act. Any termination or dissolution of the employment contract should be assessed in an individual case on the basis of whether absence from work has been unjustified e.g. on the basis of Employment Contracts Act.

An employer can also process an employee's health information if the employee specifically wants his or her capacity for work to be investigated on the basis of information of this kind. This means, for example, information which is of significance as regards the employee's health and

development of working conditions at the workplace or if an employee, who is unwilling to use occupational health services, wishes to investigate his or her impaired capacity for work without being completely incapable of work.

An employer is also entitled to process an employee's health information in those situations and to the extent to which it is laid down separately elsewhere in legislation, such as legislation on safety at work and occupational health. An employer can process, inter alia, statements provided by health care professionals concerning an employee's capacity for his or her job that are based on a health examination if the assessment does not contain detailed information on the diagnosis.

The aforesaid also applies to a job applicant. Job application forms must not include questions about detailed health-related information but, rather, the questions ought to be restricted in such a way that they relate to the nature of the work, bearing in mind solely the information that is of significance as regards managing the tasks.

Health information on an employee may be processed solely by those individuals who prepare decisions on the basis of the said information or enforce them. For this reason, an employer must designate the individuals who have to process health information or define the duties which involve processing of data concerning health. In order to safeguard the confidentiality of information on health, the individuals who process health information on employees are also under an obligation to maintain secrecy and may not divulge information to outsiders. The obligation to maintain secrecy also continues after the end of the employment relationship. The Act does, however, include a provision according to which the employer may submit the medical certificate given to him by the employee to the occupational health care for the implementation of occupational health care, unless the employee has prohibited any submitting.

An employee's health information must be kept separately from other personal data collected by an employer. Sensitive data must be removed from the personal data file as soon as there is no ground for examination and the need for retaining information has to be assessed by the employer in any case at least every five years (Personal Data Act, § 12(2)).

If an employer or its representative deliberately or through gross negligence processes information on an employee's health in a manner contrary to the aforesaid and thereby violates the protection of the employee's privacy or causes him or her other damage or fundamental inconvenience, he or she shall be sentenced to a fine or to a maximum of one year's imprisonment for a person register offence (Penal Code, Chapter 38, § 9).

Processing personal credit data

Since the importance of personal credit data has also increased in working life, it has been deemed necessary to enact rules for processing such data. The new provision defines the grounds under which the employer has the right to process personal credit data concerning a job applicant or an employee for the purposes of establishing his or her reliability.

This amendment to the Act entered into force on 1 September 2008.

The employer has the right to obtain and use personal credit data concerning a job applicant who has already been selected for the job or an employee who changes jobs while remaining employed

by the same employer, where the duties in question require a particular level of reliability and involve the possibility to seek unlawful financial benefits.

The employer's right to use the personal credit data of a job applicant are limited to duties:

- which include decision-making power or independent discretionary power to make significant financial commitments;
- in which the task is to issue and monitor financially significant credits;
- for the fulfilment of which the employer grants access to the employer's or its customer's protected business or professional secrets;
- the fulfilment of which requires access rights to an information system enabling the user to transfer the employer's or its customer's funds or to modify the related data;
- which fundamentally consist of handling money, securities or valuables in quantities of significant value, without direct supervision;
- which consist of guarding the employer's or its customer's property; or
- where their nature principally involves unsupervised work in a private home.

The employer shall always be responsible for any expenses incurred from collecting personal credit data, even in cases where the employee submits such data to the employer upon the latter's request. Where the employer collects said personal credit data, it must notify the employee from which register the data has been received. This provision also affects the operations of companies providing credit data: they are allowed to disclose employee credit data to an employer only pursuant to the grounds referred to in the Act.

An employer or his/her representative who, deliberately or through gross negligence, obtains or uses an employee's personal credit data and thereby violates the Act, shall be sentenced to a fine for violating the Act on the Protection of Privacy in Working Life.

Processing information on drug use (§ 6 - § 12)

An employer's right to process certificates concerning drug tests

The Act includes provisions on the right of an employer to process data entered in certificates on drug tests, not the actual drug tests. The provisions start from the assumption that the job applicant or employee himself submits the certificate on the drug test to the employer. The certificate must only show that a drug test has been made to the employee and that a clarification has been made as to whether he has used drugs for other purposes than medical ones so that his working capacity has become deteriorated. The definition of drug is the same as in the Drugs Act to which the Act refers. Since the data on drug tests is sensitive health information, the same restrictions of the right of retaining, confidentiality and handling are applied to its processing as to other health information.

Submitting of certificates on drug tests during recruitment

An employer is entitled to ask *the person chosen for the job* for a certificate on a drug test. A job applicant is not obliged to submit a certificate. The employer may, however, when considering to employ a person not take into consideration a job applicant who does not submit the certificate to the employer. Thus the selection will probably in practice be conditional until the person chosen for the task has submitted the certificate. As for civil servants and holders of an office, the submitting of the certificate may be a prerequisite for the appointment to the office.

The right to process the data entered into the certificates on drug tests is based on the preconditions for the right of processing, based on work tasks, and laid down by law. For this reason, data based on general sifting tests must not be processed. The employer may ask for a certificate on a drug test, if the purpose if that the job applicant shall work in such tasks which require accuracy, trustworthiness, independent judgement or a good capacity to respond. These requirements mean stricter preconditions than the general obligation to work carefully, related to the employment relationship of an employee or a civil servant.

A further precondition is that certain non-desired effects may according to general experience be caused by persons, who manage the task exposed to drugs or dependent of them. The tasks must be of a kind where their implementation exposed to drugs or dependent of drugs may

- endanger the life, health or occupational safety of the employee or some other person,
- endanger national defence or the safety of the state,
- endanger traffic safety,
- increase the risk of significant environmental damages,
- endanger the data security of information received when working, and thus cause damage to the public interest protected by secrecy provisions, or endanger the protection of the privacy or rights of those registered, or
- endanger business or professional secrets or cause greater economic damage than minor one to the employer or his customers, unless endangerment or the arise of risks can be avoided by other means.

The Act also includes a special provision for certain special situations where it is possible to ask for a certificate on drug tests.

Provisions on the employee are also applied in situations where the tasks of a person in an employment relationship or a civil servant's employment relationship are altered so that they meet the preconditions described above on the employer's right to process the certificate on drug tests.

Submitting a certificate on drug tests during an employment relationship

During an employment relationship or a civil servant's employment relationship, the employer may oblige the employee to present a certificate on drug tests. The obligation to submit the certificate is mainly an obligation related to the employment relationship, the violation of which may cause sanctions for the employee, which are determined on grounds pertaining to labour and official law on the basis of overall consideration.

The employee is obliged to present a certificate on drug tests, when it is justified to suspect that the employee is working exposed to drugs or that the employee is dependent of drugs. It is also required that the testing is necessary in order to find out the working capacity and that the employee works with tasks which require special accuracy, trustworthiness, independent judgement or good capacity to respond, and that the performing of the tasks under exposure to drugs or dependent of drugs either seriously endanger the life or health of the employee, or could cause other significant damage. The same interests as at recruitment are to be protected, yet the criteria are clearly more severe. The employer may also set a reasonable time limit for the employee, during which the certificate must be presented.

The employer may also oblige the employee to present the certificate, when the employee, having received a positive test result, has committed himself to medical care.

The employer's obligation to give notification on a certificate on drug tests, and the costs for supplying a certificate.

The employer is under an obligation to notify the job applicant, even before the making of an employment contract, of the fact that it is a question of a task where he requests the person chosen or obliges the employee during the employment relationship to present a certificate on drug tests.
The employer is responsible for the costs caused by the certificate on drug tests of both the job applicant and the employee.

Relation to the provisions on health examinations

In occupational health care, drug tests can be made to an employee or a job applicant on the basis of the Occupational Health Care Act. Then the occupational health legislation is applied to the performing of the tests, and thus every need for a test is assessed by a health care professional, not by the employer. Nor can the test result be given to the employer, only a general clarification on the health condition pertaining to the working capacity may come into question. On the basis of the special legislation on civil servants, the drug tests can also be part of the health examination on the basis of the legislation on civil servants.

Other provisions related to drug tests

The provisions do not apply to professional athletes in employment relationships, since the athletes have their own regulations on doping tests.

An employer or his representative, who deliberately or of gross negligence receives or otherwise processes data entered into the job applicant's certificate on drug tests, or demands against the provisions of law the employee to present a certificate on drug tests, may be sentenced to a fine for violating the Act on Data Protection in Working Life.

In connection with the enactment of the Act, a provision has been added to the Occupational Health Care Act concerning the employer's obligation to make a written comprehensive action programme on alcohol and drugs in cooperation with the personnel. The programme should include the general objectives of the working place and the practices to be observed to prevent the use of alcohol and drugs and to assign those with alcohol and drugs problems to receive care. Without such a programme, no testing must be performed.

The Occupational Health Care Act also includes a provision, according to which a positive test result always has to be ensured in a laboratory where quality is supervised.

The *legislation on cooperation* includes provisions stating that work tasks where the employer intends to request or require a certificate on drug tests have to be treated according to the cooperation procedure. Unless the cooperation legislation is not applicable, the employer must, before determining the comprehensive action programme on alcohol and drugs, give the employees or their representatives a chance to be consulted on the task-specific grounds for drug tests.

Requirements concerning the performance of tests and examinations (§ 13 - § 15)

Personality and aptitude assessment

The personal characteristics and knowledge and skills of job applicants and employees are assessed by means of various personality and aptitude assessments.

A job applicant or employee can be tested only if he or she gives his or her consent for this. Tests can be conducted if their purpose is to determine prerequisites for carrying out tasks or the need for training or other professional development. In accordance with the aforesaid, the results obtained by means of tests should be directly necessary as regards the employment relationship of each employee. This requirement in fact restricts both the content of tests and their scope, since there are differences in requirements between different professions and tasks.

As an employer uses information obtained by means of testing for decision-making relating to an individual employee, the results of the tests must be flawless. In order to secure this, the employer has a duty to ensure that tests are carried out using reliable testing methods, that the people conducting them are experts and that the data obtained with the testing are free from error. However, as assessment based on behavioural sciences is usually involved here, the absolute flawlessness of the data cannot be required. For this reason, any assessment of the employer's responsibility has to take the testing method and its character into account.

An employer has a variety of means at his or her disposal for determining from the available alternatives a test that is suitable for a given purpose, and for ascertaining the expertise of the person conducting it. He or she can

- resort to expert assistance or
- opt for a selection by determining the qualifications of whoever is to conduct the test
- base his or her choice on the generally known expertise of the company performing the tests
- determine in advance how and where the test has been developed and by whom and what it can actually ascertain and with what degree of probability
- ask to see an example of a written statement and feedback compiled by the tester.

The guidelines of the International Labour Organisation (ILO) note that graphological, astrological and other comparable tests ought to be excluded.

The employer or tester must provide a job applicant or employee with the written statement compiled in the personality and aptitude assessment upon request and without charge. If the statement has been given orally to the employer, it can also be given orally to the employee. The employer is ultimately responsible for the employee receiving the statement.

An employer or his/her representative who, deliberately or through gross negligence, tests an employee using personality and aptitude assessments without that person's consent or fails to ensure the reliability of the testing method, the expertise of the tester or the data obtained by means of the tests is free from error, or does not pass the statement to the employee, can be ordered to pay a fine for violating the Act on Data Protection in Working Life.

Use of health care services

In order to guarantee the legal protection of employees, an employer may only use health care professionals, people with the appropriate laboratory qualifications and health care services whose operating prerequisites, qualification requirements, obligation to maintain secrecy etc. are laid down in the legislation on both public and private health care for carrying out examinations relating to an employee's health or for taking samples. If an employer uses people or services other than the aforesaid, he or she is to be ordered to pay a fine for violating the Act on Data Protection in Working Life.

The obligation to use health care services also applies to alcohol and drug tests.

The provision does not alter or extend an employer's rights, for which reason the health care professionals determine the measures and examinations necessary for clarifying the health of the employee.

The emphasis in health care decisions is on the patient's free will, something which also applies to work-related health care. However, there are also situations in which an employee is under an obligation to take part in health check-ups. Provisions on these are to be found in, inter alia, the Occupational Health Act and the Contagious Diseases Act. The special requirements imposed by the job can also call for health check-ups as in, for example, jobs in transportation, the police, fire and rescue services. There are also special provisions for determining the health of officials.

Genetic testing

An employer must not require a job applicant or an employee to take part in genetic testing. Nor is an employer entitled to know whether an employee has taken part in genetic testing at some point in his or her life or whether the information on the health situation of the employee is based on genetic testing

Genetic testing refers to all genetic investigations including prognostic gene tests involving examinations of the relatives of individuals with hereditary diseases.

If, contrary to the provision, an employer or his or her representative requires an employee to take part in genetic testing or obtains information about genetic testing performed on an employee, he can be ordered to pay a fine for violating the Act on Data Protection in Working Life.

Camera surveillance at working places (§ 16 - § 17)

Preconditions for camera surveillance

The law provides on the right to implement camera surveillance in premises where employees are working, although the purpose of the observation were not the surveillance of the employees. The employer may conduct camera surveillance, if the purpose of the observation is to ensure the personal safety of the employees and other persons working in the premises, to protect property or supervise the adequate operations of productional processes, or to prevent or clarify situations endangering safety, property or productional processes.

As a rule, camera surveillance must not be used for observing a certain employee or certain employees at the working place. There must not be any camera surveillance in the toilets, locker rooms or social premises of the employees. It is also prohibited in working rooms which have been assigned for the personal use of the employees.

If camera surveillance is necessary, it can, however, be focused on a certain place of work, where there are employees working, if

- its purpose is to prevent apparent threat of violence related to the work of the employee, or apparent disadvantage or danger to his safety or health, or
- observation is necessary for preventing and clarifying crimes against property, if an essential part of the employee's tasks consists of handling property that is significant as to its value or quality, such as money, bonds or valuables, or
- the interests and rights of the employee should be secured, if the camera surveillance is based on the request of the employee.

Transparency when implementing camera surveillance

The camera surveillance should be as transparent as possible and necessary for reaching the purpose of measures. Recordings received through the surveillance may only be used for the purpose for which the observation has been conducted. Before introducing camera surveillance, clarifications should be made regarding the possibilities of using means less intervening with the privacy of the employees. § 5-7, 10 and 32-34 of the Personal Data Act shall be applied to the processing of recordings, regardless of whether they form a register of persons according to the Personal Data Act. This requires, for example, that a register specification on the matter be compiled.

After the cooperation or hearing procedure, the employees must also be notified of the beginning of the camera surveillance, its implementation and of how and in what situations the recordings are used, as well as of the placement of the cameras, if they are focused on places of work where employees are working. Information of the camera surveillance must also be provided in a perceptible way so that it shows whether it is a question of recording camera surveillance or not.

There are also certain exceptions to the commitment to the purpose of using the recordings received through camera surveillance. The recordings may be used contrary to the original purpose of substantiating the ground for terminating an employment relationship, of clarifying or substantiating disturbance, harassment or inapt behaviour referred to in the Equality Act and the Occupational Safety and Health Act, if the employer has a justified reason to suspect that the employer has been guilty of such behaviour, and of clarifying industrial accidents.

As a rule, the recordings received through camera surveillance have to be destroyed as soon as they are not necessary for implementing the purpose of the surveillance, and within a year at the latest.

If the employer or his representative requires camera surveillance contrary to a provision or violates the provisions on the transparency of camera surveillance, he can be sentenced to a fine for violating the Act on the Protection of Privacy in Working Life, unless the act at the same time fulfils the distinctive marks of illicit viewing condemned according to the most severe penal scale.

Retrieving and opening e-mail messages belonging to the employer (§ 18 - § 20)

The employer's obligations regarding necessary arrangements

Often the e-mail addresses given by the employer to be used by the employees are in the form of Christian name.surname@enterprise.fi and the sending and reading of the messages happens by means of a user name and password given to the employee. Yet, the e-mail at the working place is generally also used for personal communications not related to the employer's activities, e.g. instead of a telephone. Confidential communications cover private e-mail messages in the same way as a phone call. As a form of communications, e-mail is, however, different than a telephone, since it registers simultaneously the messages belonging to the employer as well as the employee's personal messages.

According to the provisions, the message can be opened and read by another person with the employee's consent according to the rules agreed on at the working place. This requires that the employee gives his user name and password for example to his fellow worker. The new provisions aim to give an answer to how to proceed, if the employee does not give his consent.

In order for the employer to be able to use his power, the precondition is that the employer prior to that has offered the employee different possibilities, which when being realized means that there is usually no need to touch upon the e-mail communications of his employees. One possibility is that the e-mail system sends an automatic notification of the absence and substitute of the employee to the sender of the message. Another alternative is that the messages during the absence of the employee are directed to another person or to the e-mail address used by some other employee. The offering of such possibilities requires measures from the employee himself, because the employer has no right to make such directions in the e-mail of the employee.

Although the employer would ensure the above-mentioned measures, the employee is under no obligation to use the possibilities offered. Unless the employee uses the possibilities, the employer must find out whether any messages belonging to the employer have been sent to the employee in his absence or whether he has sent messages belonging to the employer immediately before his absence. These messages must then be of a kind which the employer necessarily has to be informed of in order to finish negotiations related to his activities, for serving customers or for otherwise securing his functions. Such situations include e.g. situation in connection with orders, invoicing and complaining as well as in relevant business negotiations.

Retrieving electronic messages belonging to the employer

The assessment of whether a message belongs to the employer may in practice only happen on the basis of the information concerning the sender's identification data or the title space in the e-mail address. This information does not belong to the core substance of a confidential message. Although in most cases, it is possible to conclude from this information whether the message is private or not, this is not always possible. For this reason, the precondition for retrieving e-mail messages is additional criteria which all must be fulfilled before the e-mail is brought out:

- the employee attends to his tasks independently, which as a rule means that others do not attend to the matter at the same time
- because of the tasks or pending matters of the employee it is obvious that the above-mentioned messages have been sent to him

- the employee is absent from his work
- before beginning to open the e-mail, the employer offers the employee an opportunity to give his consent to the opening
- clarifying the matter of the message does not endure delay.

The law also includes a special provision for situations where the employee has died, or he is permanently hindered from performing his work tasks, in which case his consent to disclosing the messages cannot be had.

The employer can only use his right by means of a person using the authority of the main user of the data system. A written clarification has to be made to the employee on the retrieving of the message, unless it leads to the opening of the message. Neither must the persons involved in the retrieving of the message reveal the content of the message during the employment relationship, nor after its termination.

Opening electronic messages belonging to the employer

After disclosing the message, the message may be opened, if on the basis of the above-mentioned clarification it is obvious that it clearly belongs to the employer and fulfils the criteria described above. A precondition is also that attempts have, without results, been made to contact the sender or recipient of the message in order to find out the content of the message or to send it to another e-mail address assigned by the employer.
A written notification of the opening of the message has to be given to the employee. The same requirements concerning the persons involved in the opening and the same secrecy provisions as in the disclosure of the message also apply to the opening. The Act on the Protection of Privacy in Electronic Communications also generally includes provisions on the prohibition of taking advantage of messages not intended for the recipient.

Other provisions

If the employer or his representative contrary to the provisions retrieves or opens an e-mail message sent to an employee or sent by an employee, he may be sentenced to a fine for violating the Act on Data Protection in Working Life, unless the act at the same time fulfils e.g. the essential elements of a data break-in or a personal data file offence sentenced according to the most severe penal scale.

The Act on the Protection of Privacy in Electronic Communications (516/2004) entered into force on 1 September 2004. Beside tele-enterprises, the Act applies i.a. to community subscribers, which include enterprises and communities that handle, for example, confidential messages, identification data or the locality data of the users (e.g. employees) in their internal telephone or data net. Thus, the Act applies to employers both as parties to communications and as community subscribers. The confidentiality of the communications also applies to the identification data accruing by browsing the net pages.

The identification data consist of data produced by the communications between people. They are recorded in the e-mail servers of the enterprises themselves, in the cache memory servers of the Internet and in telephone exchanges. As a rule, the identification data are confidential. The identification data may, however, be processed e.g. for exchanging a phone call or some other

message, for invoicing or for observing technical faults. The data must be processed in a way where the protection of a confidential message or of privacy is not endangered.

Locality data are such data indicating the geographical location of a mobile which are used for locating services. The employer must not locate an employee without the latter's consent. Yet, in emergency situations, locating is always possible in cooperation with the emergency authorities.

Garbage mail consists of non-wanted text messages and e-mail communications, which jam the message systems and block the e-mail boxes. Viruses and worms are nuisance programmes, which spread via e-mail, the Internet, files and diskettes, contaminating the computers. According to the Act, it is possible for the employer without the employee's consent to prevent the reception of e-mail and text messages, and to eliminate the nuisance programmes from the messages in order to remove disturbances targeted at the data security and fight data security offences. The filtering measures can only be performed if the measures are necessary in order to secure the communications services or the communications possibilities of the recipient of the communications. At the request of the employee, the employer can always prevent the reception of disturbing garbage mail.

The filtration of garbage mail and the elimination of nuisance programmes from the messages must be done carefully, and the measures have to be dimensioned according to the severity of the disturbance to be prevented. When doing this, the protection of, for instance, confidential messages or privacy must not be restricted more than necessary.

The Act on the Protection of Privacy in Electronic Communications and compliance with the regulations given by virtue of it are supervised mainly by the Finnish Communications Regulatory Authority. The processing of locality data is supervised by the Ombudsman for Data Protection. The www.ficora.fi pages of the Finnish Communications Regulatory Authority provides information on the data protection of electronic communications and the amendments brought by the new Act.

Certain provisions and entry into force (§ 21 - § 26)

Cooperation in organizing technical monitoring and data network use

The objective of the law is to put in place at workplaces methods which relate to the purpose and introduction of technical monitoring affecting employees and are based on an employer's supervisory and monitoring right, and to the methods employed for this and to the use of electronic mail and other data networks. The law does not to establish or create for an employer any rights or obligations with regard to technical monitoring or data network use.

Technical monitoring refers, for example, to camera monitoring and access surveillance and systems for recording the processing of data and the monitoring of telephone use. The procedures also cover the use of electronic mail and a data network. Data that are collected by means of monitoring must be necessary as regards the employment relationship.

The cooperation legislation includes provisions, according to which the purpose of camera surveillance, passage control and other surveillance done by technical methods, introduction and the methods use for it as well as the use of e-mail and data networks are matters to be handled through the cooperation procedure. The cooperation procedure must be implemented before decision-

making on the matter. Fundamental changes to the monitoring method also fall within the scope of the cooperation procedure. With regard to e-mail and the other data network, the cooperation procedure mainly applies to operational rules.

In those companies and public corporations such as municipalities which the cooperation acts do not apply to, the employer should provide employees or their representatives with an opportunity to be heard before decision-making on corresponding matters.

Following the cooperation or hearing procedure, the employer must define both the purpose for which monitoring is to be used and the monitoring methods to be employed and the principles relating to the use of electronic mail and a data network. After this, the employer must make sure that employees are notified of the content of the decision.

Sanctions for violating cooperation legislation have been laid down, inter alia, in the Act on Cooperation within Undertakings. On the other hand, if an employer violates its aforesaid obligations to define and notify, he or she can be ordered to pay a fine for violating the Act on Data Protection in Working Life.

Supervision and entry into force

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

An employer must keep the Act on Data Protection in Working Life available at workplaces for employees to inspect. An employer can be ordered to pay a fine for neglecting to keep the Act available for inspection.

The Act on Protection of Privacy in Working Life enters into force on 1st October 2004. At the same time the former Act will be repealed.

Employers have been granted six months from the entry into force of the Act, i.e., until 31st March 2005, to implement the cooperation and hearing obligation regarding the openness of camera surveillance. If the other cooperation and hearing obligations have been implemented while the repealed Act was in force, no new cooperation procedure is necessary.

Act on the Protection of Privacy in Working Life

(759/2004)

Chapter 1

General provisions

Section 1
Purpose of the act

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

Section 2
Scope of application

(1) This Act lays down provisions on the processing of personal data about 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.

(2) 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.

(3) Processing of personal data is also subject to the Personal Data Act (523/1999) and the Act on the Protection of Privacy in Electronic Communications (516/2004), unless otherwise provided in this Act.

(4) Separate provisions shall be issued on the obligation of employees to undergo a health examination**.**

Chapter 2

General requirements for processing personal data

Section 3
Necessity requirement

(1) 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 relationship or with the benefits provided by the employer for the employee or which arises from the special nature of the work concerned.

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

Section 4

General requirements for collecting personal data about employees and the employer's duty to provide information

(1) The employer shall collect personal data about the employee primarily from the employee him/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 when the employer acquires personal credit data or information from the criminal record in order to establish the employee's reliability.

(2) The employer shall notify the employee in advance that data on the latter is to be collected in order to establish his/her reliability. If the employer collects personal credit data concerning an employee, the employer shall in addition notify the employee from which register the credit data is being collected. If information concerning the employee has been collected from a source other than the employee him/herself, the employer must notify the employee of this information before it is used in making decisions concerning the employee. The employer's duty to provide information and the employee's right to check the personal data concerning him/herself are also subject to other relevant provisions of the law.

(3) The collection of personal data during recruitment and during an employment relationship is governed by the cooperative procedure referred to in the Act on Cooperation within Undertakings (725/1978) and the Act on Cooperation in Government Departments and Agencies (651/1988).

Section 5

Processing health information

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

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

(3) 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.

(4) The employer must store any information in his possession concerning the employee's state of health separately from any other personal data that he has collected.

Section 5 a
Processing personal credit data

(1) The employer has the right to obtain and use personal credit data as referred to in section 4 of the Credit Data Act (527/2007) concerning a job applicant who has been selected for a job, in order to assess his/her reliability, where the job applicant would carry out duties which require a particular level of reliability and:

1) which include decision-making power to make significant financial commitments or de facto independent discretionary power in the preparation of such commitments;

2) in which the employee's specific task is to issue and monitor financially significant credits;

3) for the fulfilment of which access is granted to business or professional secrets which are essential to the employer or its customer and which are specifically protected;

4) the fulfilment of which requires access rights to an information system which enable the user to transfer the employer's or its customer's funds or to modify the related data, or in which duties the employee uses the access rights of said system's administrator;

5) which fundamentally consist of handling money, securities or valuables in quantities of significant value, without direct supervision;

6) which consist of guarding the employer's or its customer's property;

7) whose nature principally involves unsupervised work in a private home.

(2) The provisions of subsection 1 shall also apply if an employee's duties change during the employment contract in such a manner that they fulfil the requirements enacted in said subsection for handling personal credit data.

(3) The employer shall be responsible for expenses incurred from collecting personal credit data.

(4) Provisions concerning use rights of personal credit data in a case where an individual is selected as a person in charge in a company are enacted in section 19(2)(9) of the Credit Data Act.

Chapter 3

Processing information on drug use

Section 6
Drug test certificate

(1) The employer may only process information 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 information is otherwise subject to the provisions of section 5(2-4).

(2) 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 2 of the Narcotics Act (1289/1993) 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/her working capacity or functional capacity.

(3) 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

(1) The employer may receive or otherwise process information entered in a drug test certificate, subject to 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 quick reactions 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 business and professional secrecy or cause more than a minor level of financial loss to the employer or a customer of the employer, provided that this could not be prevented by other means.

(2) The employer also has the right to process information 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.

(3) 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 information entered in a drug test certificate.

(4) 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 comprehensive action programmes on alcohol and drugs are laid down in section 11 of the Occupational Health Care Act.

Section 8
Submission of a drug test certificate during the employment relationship

(1) The employer may require the employee to present a drug test certificate during his/her employment relationship if the employer has justifiable cause 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 essential 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 quick reactions 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 business and professional secrecy of financial significance or could cause a significant financial loss to the employer or a customer of the employer, provided that this could not be prevented by other means; or

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 2 of the Narcotics Act.

(2) The employer may impose on the employee a reasonable deadline within which the certificate must be presented. Provisions on comprehensive action programmes on alcohol and drugs are laid down in section 11 of the Occupational Health Care Act.

(3) The employer also has the right to process information 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 information in the certificate is related to monitoring progress with 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/her contract, that the nature of the job is such that the employer intends to process the information 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 him.

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 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

Requirements concerning the undertaking of tests and examinations

Section 13
Personality and aptitude assessments

(1) With the employee's consent, he/she can be tested by means of personality and aptitude assessments to establish his/her capacity to perform the work in question or his/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 error-free, the assessment method used and the nature of the assessment method must be taken into account.

(2) 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

(1) When carrying out employee health examinations and tests and taking samples, health care professionals, properly trained laboratory personnel and health care services must be used as laid down in the health care legislation.

(2) 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

(1) The employer may operate a system of continuous surveillance within his 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.

(2) Notwithstanding subsection 1, the employer may, however, direct the camera surveillance at a particular work location in which 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 and the matter has been agreed between the employer and the employee.

Section 17
Transparency when implementing camera surveillance

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

1) the potential for using other means that interfere less with the privacy of employees is investigated 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) the use and other processing of recordings of people obtained through surveillance is planned and performed with due consideration to the provisions of sections 5-7, 10 and 32-34 of the Personal Data Act, irrespective of whether the recordings constitute a personal data file under that Act;

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(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.

(2) Notwithstanding subsection 1(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) or harassment and inappropriate behaviour as referred to in the Occupational Safety and Health Act (738/2002), provided

that the employer has a justifiable reason to suspect that the employee is guilty of harassment, molestation or inappropriate behaviour; or

3) investigating an occupational accident or some other situation causing a danger or threat referred to in the Occupational Safety and Health Act.

(3) 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 deadline 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

Retrieving and opening electronic mail messages belonging to the employer

Section 18
The employer's obligations regarding necessary arrangements

(1) The employer has the right to retrieve and open electronic mail messages sent to an electronic mail address allocated by him 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/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/her consent to an arrangement whereby in his/her absence another person of his/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 his operations or the appropriate organization of the work.

(2) 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

(1) 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/her absence, been sent, or has sent or received immediately before the absence, messages belonging to the employer about which it is otherwise essential that the employer has information in order to complete negotiations concerning his operations or to serve customers or safeguard his operations, 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/her duties, and messages belonging to the employer cannot be obtained for his use despite the fact that the employer has seen to his 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.

(2) If the employee has died or if he/she is prevented in a permanent way from performing his/her duties and his/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 him, unless finding out about the matters attended to by the employee and safeguarding of the employer's operations is possible by other means.

(3) If message retrieval does not lead to opening of the message, a report must be drawn up accordingly, signed by the persons involved and stating why the message was retrieved, the time it was retrieved and who performed the retrieval. 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 its termination.

Section 20

Opening of electronic messages belonging to the employer

(1) 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 his operations or to serve customers or safeguard his 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.

(2) 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(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 its termination.

(3) The person employed by the employer or a person acting on the instruction of the former, to whom the employee has directed his/her electronic mail in the manner referred to in section 18(1)(2) or who can, in the manner referred to in section 18(1)(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/her consent to another procedure.

Chapter 7

Miscellaneous provisions

Section 21
Cooperation in organizing technical monitoring and data network use

(1) 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, are governed by the cooperative procedure referred to in the Act on Cooperation within Undertakings and the Act on Cooperation in Government Departments and Agencies. In undertakings and in organizations 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.

(2) After the cooperative 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
Supervision

Compliance with this Act shall be supervised by the occupational health and safety authorities together with the Data Protection Ombudsman.

Section 23
Display

The employer shall display this Act for employees to view at the workplace.

Section 24
Penal provisions

(1) An employer or his representative who deliberately or out of gross negligence

1) violates the provisions of sections 4(2) or 9 on the duty to provide information;

2) collects or uses a job applicant's or employee's personal credit data, contrary to the provisions of section 5 a;

3) receives or otherwise processes information entered in a job applicant's drug test certificate, contrary to the provisions of section 7;

4) requires the employee to present a drug test certificate or otherwise processes information entered in such a certificate, contrary to the provisions of section 8;

5) subjects the employee to personality or aptitude assessments without his/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(1);

6) violates the provisions of section 13(2) on provision of a written statement or provision of information on the content of an oral statement;

7) uses other than health care professionals, properly trained laboratory personnel or health care services, contrary to the provisions of section 14;

8) 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;

9) introduces camera surveillance, contrary to the provisions of section 16;

10) violates the provisions of section 17 on the transparency of camera surveillance;

11) 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;

12) violates the provisions of section 21(2) on the duty to determine and inform; or

13) 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.

(2) The penalties for a personal data file offence, computer break-in, illicit viewing, eavesdropping, message interception, violation of a confidentiality obligation, and an offence in public office are laid down in the Penal Code (39/1889).

Chapter 8

Entry into force

Section 25
Transitional provisions and entry into force

(1) This Act enters into force on 1 October 2004.

(2) If the employer's obligations laid down in sections 4(3) and 21 of this Act are met in the manner laid down in sections 4(3) and 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

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

(2) If another act or decree contains a reference to the Act on the Protection of Privacy in Working Life that was in force at the time of the entry into force of this Act, the present Act shall instead apply.

Act Amending the Occupational Health Care Act
(760/2004)

Section 3
Definitions
For the purposes of this Act:

6a) *drug test* means a test performed to ascertain the use of a drug referred to in section 2 of the Narcotics Act (1289/1993) and a report based on the test stating whether the job applicant or employee has used drugs for non-medicinal purposes;

Section 9
Compensation for the costs of occupational health care

---

(2) The provisions of subsection 1 do not apply to the costs incurred in performing drug tests.

Section 11
Occupational health care action plan and comprehensive action programme on alcohol and drugs

---

(4) If a job applicant or employee is to undergo a drug test referred to in section 3(1)(6a), the employer must have a written comprehensive action programme on alcohol and drugs, which must include the general goals of the workplace and the practices to be complied with in order to prevent the use of alcohol and drugs and to direct alcohol and drug abusers for treatment. The action programme may form part of the occupational health care action plan. Before the action programme can be approved, the jobs concerned must be discussed within the cooperation procedure as provided in the Act on Cooperation within Undertakings (725/1978) and the Act on Cooperation in Government Departments and Agencies (651/1988). In undertakings and in organizations 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 about the criteria for drug tests in each of the jobs concerned.

Section 13
Duty of employee to attend a medical examination

---

(3) A general assessment of the employee's state of health in relation to his or her duties or the duties planned for him or her must be entered in the certificate that is provided on the basis of the medical examination referred to in subsection 1(2) above.

Section 19
Drug tests and drug test certificates

(1) A positive test result obtained from a drug test on a job applicant or employee shall be confirmed at a quality-controlled laboratory. Notwithstanding provisions laid down elsewhere in the law, the person tested is always entitled to a written copy of the test result.

(2) Provisions on the content of drug-test certificates are laid down in the Act on the Protection of Privacy in Working Life (759/2004). The certificate must be given to the person who was tested, who will then convey it to the employer.

(3) Further provisions on quality control of drug tests and on taking, analysing and interpreting samples necessary for the tests in a manner that accords with good occupational health care practice and with laboratory quality standards may be given by Government decree.

———————

This Act enters into force on 1 October 2004. The employer obligations laid down in section 11(4) of the Act must be met within six months of the Act's entry into force.

Act Amending Section 6 of the Act on Cooperation within Undertakings
(761/2004)

Section 6
Matters covered by the cooperation procedure

The matters covered by the cooperation procedure are as follows:

8a) the purpose, implementation and methods used in employee monitoring performed using camera surveillance, access control and other technical methods, and the use of electronic mail and data networks;
8b) prior to the approval of a comprehensive action programme on alcohol and drugs referred to in section 11(4) of the Occupational Health Care Act (1383/2001), the tasks referred to in sections 7 and 8(1) of the Act on the Protection of Privacy in Working Life (759/2004), about which the job applicant or employee is obliged to provide, or may consent to provide, a drug test certificate to the employer;

This Act enters into force on 1 October 2004.

Act Amending
Section 7 of the Act on Cooperation
in Government Departments and Agencies
(762/2004)

Section 7
Matters covered by the cooperation procedure

The matters covered by the cooperation procedure are as follows:

11a) the purpose, implementation and methods used in employee monitoring performed using camera surveillance, access control and other technical methods, and the use of electronic mail and data networks;
11b) prior to the approval of a comprehensive action programme on alcohol and drugs referred to in section 11(4) of the Occupational Health Care Act (1383/2001), the tasks referred to in sections 7 and 8(1) of the Act on the Protection of Privacy in Working Life (759/2004), about which the job applicant or the applicant for a civil service post or the employee or the civil servant is obliged to provide, or may consent to provide, a drug test certificate to the employer;

_____

This Act enters into force on 1 October 2004.

Act Amending
Sections 8b and 19
of the State Civil Servants Act
(763/2004)

Section 8b

A precondition for appointment to a civil service post is that the person who has applied for the post or senior position must, at the request of the authority, provide information about his or her state of health in relation to performance of the duties in question and also, where necessary, undergo examinations and tests in order to clarify the matter. The person who has applied for the post or senior position can be required to supply a drug test certificate in situations referred to in section 7 of the Act on the Protection of Privacy in Working Life (759/2004) as a precondition for appointment to a civil service post. The provisions of section 19(2) apply to the payment of costs incurred in the examinations and tests.

Section 19

At the request of the authority concerned, a civil servant is required to provide the authority with any information about his or her state of health in relation to performance of the duties in question. A civil servant may also be ordered to undergo examinations and tests to establish his or her state of health if this is necessary to ascertain whether he or she is fit to perform his or her duties. The provisions of section 8 of the Act on the Protection of Privacy in Working Life apply to the right to require a civil servant to supply a drug test certificate.

_____

This Act enters into force on 1 October 2004.

Act Amending
Sections 7 and 19
of the Act on Civil Servants in Local Government
(764/2004)

Section 7
Establishing state of health

A precondition for employment as a municipal officeholder is that, at the request of the authority, the person to be employed provides information concerning his or her state of health in relation to performance of the duties in question to the authority making the employment decision, and, where necessary, also undergoes examinations and tests in order to clarify the matter. A person to be employed as a municipal officeholder can be required to present a drug test certificate in situations referred to in section 7 of the Act on the Protection of Privacy in Working Life (759/2004) as a precondition for appointment as a municipal officeholder. The necessary costs incurred in the examinations and tests ordered by the employer will be met by the employer.

Section 19
Provision of health information

In addition to the provisions of the Occupational Health Care Act (1383/2001), a municipal officeholder is required, at the request of the employer, to provide the latter with the necessary information concerning his or her state of health in relation to performance of the duties in question in order to establish his or her working and functional capacity. A municipal officeholder is also required, on the order of the employer, to undergo examinations and tests to establish his or her state of health if this is necessary to ascertain whether he or she is fit to perform his or her duties. Before issuance of the order, the municipal officeholder shall be reserved an opportunity to be consulted. Provisions of the Act on the Protection of Privacy in Working Life apply to the right to require a civil servant to present a drug test certificate. Provisions on a patient's right of self-determination are laid down in section 6 of the Act on the Status and Rights of Patients (785/1992).

_____

This Act enters into force on 1 October 2004.

TEM/TSA 20.10.2008