DATA PROTECTION INSPECTORATE

GUIDELINES FOR HUMAN RESOURCES EMPLOYEES:

PERSONAL DATA IN EMPLOYMENT RELATIONSHIPS

Approved on 6 June 2011

Introduction

- **Who are the guidelines meant for?**

These guidelines are primarily meant for the **human resources managers of companies.**

The **guidelines** give an overview of the rules of **processing the personal data of employees** and **job applicants** given in the guidance notes[1] approved by the Data Protection Inspectorate on 24 January 2011.

The guidelines are applied to employment relationships based on **employment contracts.**

- **What is personal data processing?**

Any activity done with the data of a natural person is personal data processing.

Even the collection of personal data alone is personal data processing, but it also includes saving, storage, forwarding and disclosure, destruction of personal data, etc.

Personal data are any data about an identified or identifiable person irrespective of the shape or form of such data.

- **Who processes personal data?**

An employer is always a controller (or processor) of personal data, because the employee's name and identity code alone are personal data.[2]

An employer is a data controller even when they are still recruiting employees.

- **Where do the rules come from?**

Subsection 41 (2) of the Employment Contracts Act stipulates that an employer must process the personal data of an employee pursuant to the Personal Data Protection Act.

The Personal Data Protection Act regulates who may process the data of other people and under what conditions they may do so. The Personal Data Protection Act also applies to employers.

The Data Protection Inspectorate gives advisory guidelines about personal data processing.

---

[1] Comprehensive Guidance Notes about processing personal data in employment relationships. Available only in Estonian.

[2] English translation of Estonian Data Protection Act (available at http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=XXXX041&keel=en&pg=1&ptyyp=RT&tyyp=X&query=isikuandmete) uses „chief processor“ for controller and „authorised processor“ for processor.

Table of Contents

Chapter 1. PROCESSING THE DATA OF JOB APPLICANTS

Is the consent of a job applicant required for the collection of data about them?

1. The personal data of a person applying for a job may be processed on the basis of their consent.[3]
2. Consent is not necessary if the employer is obliged to collect certain data about the applicant pursuant to law;
    - for example, the Communicable Diseases Prevention and Control Act prescribes the cases where an employer must request that the person to be hired submit a written health certificate.
3. The separate consent of an applicant is not required for processing the data submitted by themselves to the employer.
    - The applicant's consent to the employer contacting the reference providers noted in the CV may also be presumed.
4. No consent is required for the collection of data disclosed pursuant to law or by the applicant themselves;[4]
    - disclosure means making data accessible to an undetermined circle of people (e.g. an employee's blog on the Internet);
    - disclosure to the circle of people determined by the applicant themselves on the Internet is not disclosure;[5]
    - data entered in the Commercial Register, official notices, court rulings, etc., are data disclosed on the basis of law.
5. The applicant's consent is required for collection of data from non-public sources;[6]
    - for example, when requesting a reference from a previous employer;
    - also when requesting data from existing employees and acquaintances.
6. Applicants may not be required to submit extracts of their criminal record.
7. Employers can request data from the Punishment Register themselves as stipulated in the Punishment Register Act:
    - until 31 December 2011, an employer may request a certificate from the Punishment Register that confirms whether or not the applicant complies with the requirements set for the job by law;
    - from 1 January 2012, every employer may request an extract about every applicant from the Punishment Register.

What must be written in the consent?

The Personal Data Protection Act establishes the requirements for the content and format of the consent.[7]

1. The consent must be in a format that can be reproduced in writing;

---

[3] Clause 2.1. of the Guidance Notes.
[4] Clause 2.1.6. of the Guidance Notes.
[5] E.g. the applicant's friends in a social networking portal.
[6] Clause 2.1.7. of the Guidance Notes.
[7] § 12 of the Personal Data Protection Act.

- for example, e-mail, fax, copy of a signed document (incl. electronic copy in pdf format) are formats that can be reproduced in writing.
- formal requirements stricter than the ones stipulated by law may always be followed, i.e. the consent may be obtained in written format (bearing the applicant's hand-written signature) or electronic format (digitally signed).

2. If the consent is obtained together with another expression of will, the consent to personal data processing must be given separately;
3. silence or inactivity is not regarded as consent;
4. the consent may be partial and conditional;
5. in the event of a dispute, the employer must prove that a consent existed;
6. the general requirements set forth in the Personal Data Protection Act must be observed even when data are processed on the basis of a consent (see clause 2.3. of the guidelines);
7. consent may only be given for the processing of a person's own data and the data of their underage children;
8. a consent may be withdrawn at any time, but withdrawal has no retroactive effect.
9. The following must be clearly determined in the consent:
    - the data for which the permission to process is given;
    - the purpose for which data are processed;
    - the persons to which communication of the data is permitted;
    - the terms of communicating the data to third parties;
    - the rights of the data subject in regard to the further processing of their data.

See also the sample consent form on the website of the Data Protection Inspectorate!

What may be requested from an applicant?

1. There must be legitimate interest in the data required from an applicant;[8]
    - the recruitment agencies used to recruit employees may also not request data in which the employer has no legitimate interest;
    - legitimate interest must be assessed on the basis of the specific employment relationship and the requirements for the position to be filled;
    - lack of a legitimate interest is mainly presumed in the case of questions that show a disproportionate interest in the applicant's private life;
    - there must be a legitimate interest in the requested information irrespective of how the data are requested – for example, also if the job advert already listed the data or documents that applicants must submit;
    - the requirement for legitimate interest also applies to requesting sensitive personal data from applicants.[9]
2. Requesting data and documents necessary for the performance of an employment contract during an employment relationships is not justified at the recruitment stage.
3. Testing (e.g. testing mental abilities and personal traits) is also personal data processing.

[8] § 11 of the Employment Contracts Act. Clauses 2.1., 2.1.1. of the Guidance Notes.
[9] Clauses 2.1.4 . and 2.1.5. of the Guidance Notes.

- Testing may be done with the applicant's consent and provided that there is a legitimate interest in the data obtained as a result of the test.
- In the event of automated testing, the applicant must be given the opportunity to submit objections if the applicant is not chosen as a result of the test.[10]

4. An employer may demand a health check or a drug or alcohol test if there is a legitimate interest in such data and the applicant gives their consent.
   - Requesting such data from all applicants at the initial stages of application is certainly not justified.[11]

Does an applicant have the right to ask what data have been collected about them?

1. An applicant has the right to know which data the employer has collected about them, the purpose for which the data were collected and the person to whom they were communicated.[12]
2. An applicant has the right to view the collected data.
3. Data about other applicants may not be given.
4. If a recruitment agency is used, the contact details of both the recruitment agency (the data processor) as well as the company itself (the data controller) must be given to the applicant.

How long may the data of an applicant be preserved?

1. The data collected about an applicant may be preserved until the deadline for disputing the recruitment decision has expired.[13]
2. The consent of the applicant is required for further preservation of the data or their processing for any other purposes.

Recommendations

- If you ask an applicant to fill in an application form, mark the questions in which the company has a legitimate interest and the questions the applicant may answer if they want to.
- It is often difficult for applicants to decide whether or not the company has a legitimate interest in certain circumstances. In order to avoid a misunderstanding, be ready to justify how a question relates to the requirements set to the job.
- You want to find out whether the applicant's health allows them to do the job you offer? Instead of asking whether the applicant has one illness or another, list the illnesses or circumstances that pose an obstacle and ask the applicant to

[10] § 17 of the Personal Data Protection Act. Clause 2.1.8 of the Guidance Notes.
[11] Clause 2.1.5 of the Guidance Notes.
[12] Clause 2.2 of the Guidance Notes. The right of an applicant to review personal data is regulated by § 19 of the Personal Data Protection Act. Pursuant to the Equal Treatment Act, an applicant who was not hired has the right to file a claim for damages against the employer within 1 year.
[13] Clause 2.3. of the Guidance Notes.

confirm that they are not suffering from any of these. Separate confirmation about every illness or circumstance may not be requested.

- You could use a similar method if the obstacle is the fact that someone close to the client works for a competitor.
- Prepare a privacy policy and publish it on your website, and include an explanation of the terms of processing the personal data of the persons who apply for jobs. See the Privacy Policy of the Data Protection Inspectorate![14]

[14] "How do we keep your private information?" www.aki.ee. Available only in Estonian.

Chapter 2. PROCESSING THE PERSONAL DATA OF EMPLOYEES DURING EMPLOYMENT RELATIONSHIPS

2.1. Processing without consent

The consent of an employee need not be requested if the personal data of the employee are processed in the following cases: [15]

1. the employee's personal data are processed to the extent and under the terms prescribed in the employment contract for the performance of the employment contract;[16]
   - the work organisation rules established by the employer that are mentioned in the employment contract are also a part of an employment contract;
   - such processing of personal data that is in contravention to the Personal Data Act or other laws, the principles of good faith, good morals or public order cannot be prescribed in the employment contract or the rules of work organisation;
   - however, sensitive personal data may not be processed for the purpose of contract performance or guaranteeing such performance. Data about intoxication are also sensitive personal data.
2. The obligation to process personal data arises from law;
   - for example, the Occupational Health and Safety Act stipulates that an employer must participate in the investigation of an occupational accident and therefore also process the health data of an employee to the extent prescribed by law;
3. the personal data of an employee are forwarded to institutions that need them for the performance of their duties arising from law;[17]
   - for example, an employer gives the data of an employee to the Tax and Customs Board in relation to social and income tax;
4. the personal data of an employee that the employee has disclosed themselves are processed;[18]
   - disclosure means making data accessible to an undetermined circle of people (e.g. an employee's blog on the Internet);
   - disclosure to the circle of people determined by the employee themselves on the Internet is not disclosure;[19]
5. the personal data of an employee that were disclosed on the basis of law are processed;[20]
   - for example, data entered in the Commercial Register, official notices, court rulings;
6. surveillance equipment is used to protect persons and property;[21]

[15] Clause 1.3.1. of the Guidance Notes.
[16] Clause 14 (1) 4) of the Personal Data Protection Act.
[17] Clause 14 (2) 1) of the Personal Data Protection Act.
[18] Subsection 11 (1) of the Personal Data Protection Act.
[19] E.g. the employee's friends in a social networking portal.
[20] Subsection 11 (1) of the Personal Data Protection Act.

7. it is necessary to process personal data in an exceptional situation to protect the life or health (but not property!) of an employee or another person and the employee's consent cannot be obtained.[22]

2.2. Processing on the basis of consent

1. The personal data of an employee may be processed on the basis of a consent during an employment relationship only if:
   - it is actually possible for the employee to decide whether or not they give their consent;
   - it is possible to end the processing if the employee withdraws their consent.
   - For example, a photo of the employee may be displayed on the company's website with the employee's consent.
2. Asking for consent is misleading if processing is unavoidable pursuant to law or the contract.
   - For example, it is not necessary to obtain the employee's consent if the employer asks for the personal data of the employee's child in order to grant parental leave or additional child care leave.
3. An employee may only give their consent for the processing of the employee's own data and the data of their underage children.
4. An employee may withdraw their consent at any time. Withdrawal of consent has no retroactive consequences.

2.3. Main Requirements for Processing

§ 6 of the Personal Data Protection Act stipulates that the principles of lawfulness, expediency, minimality, restricted use, data quality, security and individual participation must be considered in personal data processing. The following requirements for employers arise from these principles:

The purpose of collecting personal data

1. Personal data may be collected and processed only in an honest and lawful manner. This means that no personal data may ever be collected by covert surveillance.
2. The person who starts collecting data must think through what kind of data they will process and for what purpose. [23]
   - A large amount of an employee's personal data are constantly saved in the course of the work process, such as received and sent e-mail folders, access badge logs, security camera recordings, recently visited websites. Such collection and saving of data always done for a purpose – acknowledge these purposes to yourself and your employees!

---

[21] Subsection 14 (3) of the Personal Data Protection Act.
[22] Clause 14 (1) 3) of the Personal Data Protection Act.
[23] Clause 1.5. of the Guidance Notes.

3. The purposes of processing must arise from law or be determined in the consent to personal data processing or the employment contract (and the employer's work organisation rules mentioned therein).
4. The purpose must be determined as clearly and accurately as possible.
   - "Data processing" cannot be the purpose for which data are collected.
   - "Personal data are processed to check the employee" is not a clear enough purpose; however, "Access badge logs are used to check that employees adhere to working hours" is an acceptable purpose.
5. The same data may be collected for several purposes at the same time.
6. Personal data may only be collected in the quantity that is absolutely necessary for the purpose for which they are collected.
   - Think whether or not it is necessary to request a document from the employee, as the employee disclosing the data themselves may be enough?
   - Is it necessary to make a copy of a document, as writing certain data down may be enough?

Data storage

1. Processing must stop and data must be deleted or depersonalised when the purposes for which the personal data were collected are achieved.[24]
   - Decide on the period of time for which you need to store the data during the collection of the data.
   - The deadline for data storage may also be determined by law (e.g. employment contract for 10 years, accounting documents for 7 years).
   - If necessary, personal data may be stored after the achievement of their purpose for the duration of the disputing deadline.
   - Use automatic data deletion functions if possible!
2. Personal data are not processed in a manner that does not comply with the initial purpose of data collection, unless the employee gives their consent thereto.
   - For example, security camera recordings may not be used to prove lateness for work.

Notification of employees

1. An employee must know who processes their personal data, which personal data they process and the purpose for which the data are processed.
2. An employer must notify an employee of personal data processing at their own initiative.[25]
   - An employee must not be notified if data are processed directly on the basis of law, or if the employee has given their consent to data processing.
   - An employer must let an employee know which data the employer processes for the purpose of performance of the employment contract.
   - An employer is also obliged to notify employees if they obtain information about the employees not at their own initiative, e.g. by mistakenly opening a

[24] Clause 24 1) of the Personal Data Protection Act. Clause 4.1. of the Guidance Notes.
[25] § 15 of the Personal Data Protection Act.

private letter addressed to an employee or if someone (e.g. a bailiff) sends a query about the employee to the employer.

3. An employee is always entitled to ask which personal data their employer is processing, what the purpose is for which they are processed, and to whom they have been sent.[26]
    - An employee has the right to view the collected data.
4. The data of an employee that are stored must be accurate and up to date.[27]
    - An employee has the right to demand correction of inaccurate personal data and closure or deletion of outdated and unnecessary data.[28]

Security requirements for personal data processing

Security measures must be applied to protect personal data against accidental or unauthorised processing, disclosure or destruction.[29]

- The personal data of an employee collected by an employer must also be protected from other colleagues whose duties are not associated with personnel.

Recommendations

- Personal data protection is a complicated area. Appoint the person whose duty in your company is to prepare the personal data processing rules and check that they are adhered to. Allow this employee to attend training in personal data protection.
- Acknowledge and value employee privacy in your company.
- Make sure that the personal data processing rules are as transparent as possible. This helps create a more trusting relationship with employees, increases the company's trustworthiness and improves its reputation as an employer.
- You could prepare an information sheet that explains the terms of personal data processing simply and briefly.
- Notify employees of where and how they can view their data.
- Read also the guidelines Self-help Questionnaire of Data Protection and Data Security prepared by the Data Protection Inspectorate.[30]

2.4. Data of the Economic Interests of Employees

1. An employee may give their consent for the processing of their own data only. This means that the consent of the persons close to the employee is required for the collection of their data.
    - Instead of asking for data about the persons close to an employee, you could prepare a list of the circumstances that do not comply with the requirements for the job and ask the employee to confirm that there are no such circumstances.
2. Data collection must be purposeful and minimal.[31]

[26] § 19 of the Personal Data Protection Act.
[27] Clauses 24 2)-6) of the Personal Data Protection Act.
[28] Subsection 21 (1) of the Personal Data Protection Act.
[29] § 25 of the Personal Data Protection Act.
[30] Available only in Estonian.

- Determine the risks you want to avoid by collecting data about economic interests.
- If the purpose is to avoid conflicts of interest, define the conflict of interest and describe the activities that qualify as such. Establish the rules how an employee must behave in the event of a conflict of interest.
- Think whether the company's interests can actually be damaged in such a manner in the specific job.
- Think whether the collection of the data you wish to obtain actually achieves the desired purpose. Do you actually need the data you collect, or are you just collecting them for the sake of it?
- Consider the alternatives that are aimed at risk prevention. For example, establish job-based and document-based (technical) access restrictions to information that can be regarded as business secrets.
- Consider requesting data as an alternative only if you need to decide on a specific transaction or if there is suspicion that interests may be damaged.
- Do not burden employees with the demand to submit data that are publicly accessible (e.g. data from the Commercial Register, data from the Register of Economic Activities). You can always check these data yourself at any time if necessary.

2.5. Health Data of Employees

1. An employer has the right to demand a medical certificate in the cases stipulated by law.[32]
   - For example, a pregnant woman has the right to demand work that corresponds to their health conditions by submitting a medical certificate, which only shows the restrictions caused by the health condition.[33]
   - There is no right to demand a medical certificate if an employee visits a doctor during working hours under the terms stipulated in §§ 42 and 38 of the Employment Contracts Act.
   - If an employment contract is extraordinarily cancelled at the initiative of an employee due to their health condition, the employee must submit the reason in a format that can be reproduced in writing.[34]

2. An employer may not demand the inclusion of a diagnosis in the medical certificate or submission of medical records.
   - Even if an employer suspects that an employee has gone on holiday when incapacitated for work, the employer does not have the right to demand medical records or other medical data from the employee or the doctor.
   - An application for checking the legality of an issued certificate for sick leave may be filed with the National Health Insurance Fund.
   - It's a doctor who is entitled to assess whether or not the working conditions comply with an employee's health condition.

3. There is no right to demand submission of pregnancy records.[35]

---

[31] Clause 3.1.2. of the Guidance Notes.
[32] Clause 3.2.1 of the Guidance Notes.
[33] § 18 of the Employment Contracts Act.
[34] Clause 3.2.6. of the Guidance Notes.
[35] Clause 3.2.5. of the Guidance Notes.

- The employee will submit a doctor's or midwife's certificate in the cases provided for by law.

4. Only a decision in the format established with a regulation of the Minister of Social Affairs is submitted about the results of the health check prescribed in the Occupational Health and Safety Act.[36]

- An employer may not demand any other data or documents from the occupational health specialist.

5. An employee has the right to view the data of the employee that are processed by an occupational health specialist.

- If necessary, the occupational health specialist should explain the meaning of the abbreviations, Latin terms and numbers contained in medical documents to the employee.

6. The procedure for investigating occupational accidents and illnesses is regulated with the Occupational Health and Safety Act.

- In the event of occupational illnesses and accidents, an employer does not have the right to demand the data not specified in the Act or documents about the health condition of the employee.
- The police must be informed only about occupational accidents that resulted in death.

2.6. Data about intoxication

1. Data about intoxication are health data and therefore sensitive personal data.[37]
2. In the event of signs of intoxication, an employer has the right to process data about the employee's intoxication for the performance of the obligation arising from law (i.e. without the employee's consent).
    - An employer is obliged to remove the employee who is under the influence of alcohol, narcotic, toxic or psychotropic substances from work.[38]
    - The data of an employee's state of intoxication may also be processed by a doctor and the working environment representative due to their duties.

Recommendations

- Specify in the work organisation rules or the employment contract whether and how intoxication is ascertained in the event of signs of intoxication and how the employee is removed from work.
- Prefer a reliable method of ascertaining intoxication – let a doctor do it.

2.7. E-mail Messages

The following rules are only applied to the employer's e-mail addresses created for a single employee or containing the employee's name.[39]

[36] Clause 3.2.3. of the Guidance Notes.
[37] Clause 3.2.2. of the Guidance Notes.
[38] Clause 13 (1) 15) of the Occupational Health and Safety Act.
[39] Clause 3.4.1. of the Guidance Notes.

1. It is not prohibited for an employer to read the work-related e-mails of an employee. However, an employer must keep in mind that there may be private messages in an employee's mailbox, because:
    - incoming private e-mail can never be excluded 100%;
    - e-mails sent by colleagues to each other may have private content;
    - the content of messages may be partially private.
2. Reading e-mail in the inboxes of employees is usually done for two purposes:
    - obtaining the information that is required for the organisation of work;
    - checking employees.
3. It is not necessary for an employer to open or read the private messages of employees for the purpose of organisation of work.
4. Avoid opening private messages when looking for the information you need for the organisation of work:
    - establish rules for using the mailbox (read the recommendations below);
    - use alternative ways of getting information if possible;
    - use specific search criteria to find messages (e.g. date, sender).
5. The private messages of an employee may be read for checking an employee if all of the following conditions are met:
    - the obligation the performance of which is checked can be clearly ascertained and it is important;
    - the right to read private messages arises from the employment contract or the employee has given their consent to this;
    - the private messages contain no sensitive data;[40]
    - the performance of an obligation cannot be checked in any other manner;
    - it was reasonable possible for the other party to the message to understand that the e-mail address was not the private e-mail address of the employee;
    - the employee and the other party to the message are both notified of the message being read.
6. An employee’s e-mail must be closed immediately after the end of the employment relationship.
    - There is no need to keep it open, as the employer can set up an automatic reply, which informs the sender of a message about the mailbox having been closed and the new contact details.

Recommendations

1. Establish rules for using e-mail for employees, which help protect privacy and secrecy of correspondence of employees and third parties, and thereby reduce the company’s risks (some of the rules below exclude each other):
    - Private messages must be immediately deleted from the mailbox.
    - Private messages must be moved to a folder called ‘Private’.
    - The headings of private messages must be marked in a certain way.
    - All of the information needed for work that is obtained and sent by e-mail is saved on data media that the employee (or other employees) can access.

[40] Sensitive personal data may not be processed on the basis of clause 14 (1) 4) of the Personal Data Act, i.e. for the purpose of performance of a contract.

- The automatic out of office reply is used when the employee is not in the office.
- The employer appoints the person to whom all the e-mail sent to the employee is forwarded when the employee is away from work.
- The person, who has the right to open the employee’s mailbox when the latter unexpectedly has to stay away from work, is agreed on in advance.
- Employees may not use the e-mail address with the employer’s domain for sending private e-mail messages.
- A wizard is added to outgoing e-mail, which informs the recipient that this is the business e-mail address of the company.
- When an employment relationship ends, the employee must hand all business correspondence in the mailbox to the employer.

2. Make sure that employees know how the information relating to the mailbox allocated to the employee is processed. For example, prepare an information sheet about the following for the employee:
    - backup copies are made of mailbox contents and how long they are kept;
    - who can access backup copies and for what purpose;
    - who can obtain information from an employee’s mailbox, under what circumstances and how it can be done, and what information may be obtained;
    - if it is recorded and if yes, how;
    - when it is done (once or regularly);
    - how employees are informed of this.
3. Make sure that the employees who have access to an employee's mailbox (e.g. information system administrators) and data processors are aware of and follow the above requirements and do not disclose the private information they find in the mailbox of the employee.

2.8. Surveillance Equipment

What is surveillance equipment?

1. Surveillance equipment forwards and/or records images in order to survey a territory, people, item or process. Surveillance equipment includes GPS devices, which makes it possible to determine the location of a person or item.[41]
2. The rules described below apply irrespective of the technology used or the length of the period for which it is used.
    - All requirements apply in the same manner even if surveillance equipment is only used for a very short time, e.g. only for an hour.
3. Personal data are processed when surveillance equipment is used irrespective of whether the equipment record or survey in real time and whether or not the recordings are viewed.
4. A person is identifiable even if their face cannot be seen in the image obtained with surveillance equipment.
    - A person can be identified by their other characteristics, such as body shape, clothes, the things they carry.

[41] Clause 3.5. of the Guidance Notes.

Is the consent of an employee required for the use of security cameras?

1. The consent of an employee is not necessary if the surveillance equipment is used only for the protection of persons or property.[42]
2. Employees must be notified if surveillance equipment is used to protect persons or property.[43]
   - Employees must also be notified if the surveillance equipment is aimed at surveying clients or third parties, but employees are also in the surveyed area.
   - The notice must be clear and unambiguous.
   - The name and contact details of the person who processes data (incl. the data processor) must be given in the notice.
   - The notice may not be unreasonable far from the surveyed area.
   - Notifying persons with visual impairments must also be guaranteed if the notice is in writing.
   - Read also the recommendations for notification given below.

What restrictions apply to the use of surveillance equipment?

1. The use of surveillance equipment to protect persons or property may not damage the rights of employees excessively.
   - Sound recording is not permitted.
   - The low price of equipment is not sufficient to justify their use.
   - Read also the below recommendations on what should be considered before surveillance equipment is taken in use.
1. The security risk for which surveillance equipment is used must be clearly defined and real.
   - Surveillance equipment may not be used with a general reference to possible breaches, which may occur in the company's territory.
2. Use of surveillance equipment is not permitted:
   - in the rooms that are not meant for performance of duties, but for private use of employees, such as toilets and shower rooms, changing rooms, the lockers and rest area of employees;
   - in private offices;
   - in places where it would lead to the processing of sensitive personal data, such as trade union rooms, prayer rooms, the health worker's room and entrances to them.

Can security camera recordings be used in the event of a breach of duties?

The data obtained with the help of surveillance equipment meant for the protection of persons or property may not be used for any other purpose.[44]

---

[42] Subsection 14 (3) of the Personal Data Protection Act.
[43] Clause 3.5.2. of the Guidance Notes.
[44] Subsection 14 (3) of the Personal Data Protection Act.

Can surveillance equipment be used to check work?

Use of surveillance equipment to check the quality and quantity of the work done by employees is not permitted.

Must employees be allowed to view the recordings?

1. Employees have the right to view the data about them, incl. recordings, collected with surveillance equipment.[45]
    - Personal data must be issued to employees in human-readable format.
    - The right to view data regardless of who collected them – the employer or the security company hired by the employer.
2. An employee may request the issue of a copy for themselves, but the employer must issue data in the format requested by the employee only if possible.[46]
    - Copies may not be issued to an employee in such a manner that they contain the personal data of other persons.

Recommendations

1. Consider the following circumstances before you start using surveillance equipment:
    - What are the benefits of using surveillance equipment for the company and do these benefits outweigh the negative impact of surveillance on employees?
    - Is the purpose for which surveillance equipment is used determined clearly and unambiguously?
    - Is the intended purpose weighty enough?
    - Is the use of surveillance equipment clearly necessary? Is it an efficient means for achieving the purpose?
    - Can the purpose be achieved in another manner, without the use of surveillance equipment (e.g. by using better doors, armoured glass, locking systems and alarms with movement and other sensors to protect property)?
    - Is it definitely necessary that the surveillance equipment:
        i. record, or is surveillance in real time sufficient;
        ii. work constantly or only when a threat criterion appears;
        iii. make it possible to survey all the activities of people or a room, or is surveying just one part of the room or deciding sufficient;
        iv. be mobile or stationary;
        v. be fixed or rotate automatically or can be rotated manually;
        vi. can enlarge images;
        vii. have high resolution, which makes it possible to see details, or is a more general image, which is achieved with a lower resolution or automated rastering, sufficient.
    - Who processes the recordings or the image in real time (the employer themselves or the security company authorised by the employer)?

[45] Clause 3.5.3. of the Guidance Notes.
[46] Subsection 19 (2) of the Personal Data Protection Act.

- Are the rights of the employee who has access to the surveillance equipment or recordings clearly outlined? For example, the security employee whose duty is to survey the image in real time in the security room may not need the right to make copies of the recordings.
- Are all recordings stored, or only the ones that show security incidents?
- How long are recordings stored?

2. It is advisable to use a combined notification system to notify employees – signs are placed in the surveyed area and employees are also given a detailed document that describes the circumstances of surveillance:
    - the purpose(s) for which surveillance equipment is used (if there are several pieces of equipment and many purposes, the employer must specify the purposes for which each piece of equipment is used);
    - can the recordings made by surveillance be used to process breaches of duties and which duties does this apply to;
    - the surveyed area;
    - the time of surveillance;
    - type of surveillance (in real time or with recording);
    - general description of the surveillance equipment (stationary, rotating, can enlarge images, can record sound, etc.);
    - details of the persons who process the data collected by surveillance;
    - forwarding the data collected by surveillance to third parties;
    - organisation of protection of the data collected by surveillance;
    - the length of time for which recordings are stored;
    - the procedure for viewing recordings,
3. Careless use of surveillance equipment may do the employer more harm than good, because constant surveillance of employees with technical equipment may create an atmosphere of distrust, cause stress and humiliate employees.
4. Any filmed material creates the temptation to misuse it, which is why special attention needs to be given to the security of recordings.

2.9. GPS Devices

1. GPS devices are tracking devices. All of the requirements listed above apply to them.[47]
2. An employer may not use a GPS device to track in real time outside working hours.
3. A GPS device may be used to collect about an employee outside working hours only to the extent directly necessary either pursuant to law or for the performance of a contract.
    - Pursuant to the Income Tax Act, only the data and the initial and final readings of the car's odometer for private trips must be submitted to the Tax and Customs Board for the calculation of the fringe benefit tax.
    - The systems that record the data of the car’s location to the accuracy of time and address, and allow the employer to track the car’s location in real time, make it possible to process considerably more data than is necessary for the performance of the requirements stipulated in the Income Tax Act.

[47] Clause 3.5.1. (p. 70) of the Guidance Notes.

- An employer cannot make the use of such a system compulsory for employees, because there are alternative methods that prejudice the inviolability of private life to a considerably lesser extent.

Recommendations

1. Even when the data collected with a GPS device are not sent to the employer in real time, think of any alternatives you may find to the use of GPS devices outside working hours.
    - If the purpose is to check that the vehicle is not used for moonlighting after the end of the working day, the odometer reading can be recorded as of the start and end of the working day.
2. Similarly to other surveillance equipment, make sure that the functionality of the device makes its use proportional.
    - For example, some systems record data only in the local device, from which they are later downloaded onto a computer, and any data that are not needed are filtered out.
3. When you outsource the service, make sure that you have a clear overview of the conditions of the provided service. As the data controller, you must determine the data about your employees that the service provider processes for you as well as the purpose for which and the conditions under which the data are processed.

2.10. Equipment Based on Biometrics

1. Biometric data, such as fingerprints, images of the iris of the eye and genetic data are sensitive personal data.
2. Equipment based on biometrics is generally used in access systems, such as a laptop with a fingerprint reader or a door lock.
3. There are different types of biometric equipment:
    - equipment that saves the image (e.g. the fingerprint),
    - equipment that only saves the code created on the basis of the image.
4. Only equipment that records the code may be used on the basis of an employment contract.

Chapter 3. ACCESS TO THE DATA OF EMPLOYEES

1. Access to data also means disclosure of data and forwarding data to third parties.[48]
    - Third parties are all natural persons and legal entities and institutions that are not data processors.
    - A parent company or subsidiary is also a third party, unless they are a data processor.
    - A branch of the company is not a third party, as it is not a separate legal entity.
    - Disclosure means making data accessible to an undetermined circle of people (e.g. an employee's blog on the Internet);
    - Disclosure on a website that is only meant for registered users (e.g. the intranet of a company) is not disclosure;
2. The other employees of a company may have access to the personal data of an employee only to the extent required for the performance of the duties stipulated in the employment contract.[49]
3. A data processor processes personal data according to the instructions received from the company on the same legal basis as the company itself.[50]
    - For example a company that provides accounting or server hosting services may be a data processor.
4. The personal data of an employee may be disclosed, communicated or allowed to be accessed:
    - with the employee's consent (e.g. debt collection company, new employer, the employee's spouse);
    - if the recipient of data requests the data for the performance of the duties prescribed by law (e.g. the Tax Board, Statistics Estonia, bailiff);
    - in an exceptional situation to protect the life or health (but not property!) of an employee or another person and the employee's consent cannot be obtained.[51]
5. The personal data of an employee may not be disclosed on the basis of clause 14 (1) 4) of the Personal Data Protection Act, i.e. for the performance of a contract.[52]
6. An employee has the right to ask to whom the employer has sent their personal data.[53]

---

[48] Clause 4.2.1.2. of the Guidance Notes.
[49] Clause 4.2.2. of the Guidance Notes.
[50] § 7 of the Personal Data Protection Act. Clause 4.2.1.1. of the Guidance Notes.
[51] Clause 14 (2) 2) of the Personal Data Protection Act.
[52] Clause 4.2.1.3. of the Guidance Notes.
[53] Clause 19 (1) 5) of the Personal Data Protection Act.