Guidlines for personal data protection in employment relationships

A manual explaining the scope of employees' right to privacy and how it engages with the interests of the employers.

INFORMATION COMMISSIONER

The purpose of the document:	The purpose of the document: The guidelines provide answers to frequently asked questions of employees and employers regarding the provisions of the Personal Data Protection Act and at the same time harmonize the requirements and practices of the inspection supervision.
Target publics:	Employers and employees.
Status:	Public
Version:	1.0
Dated:	7th April 2008
Author:	Information Commissioner RS
Key words:	Guidelines, employment relationships, protection, legal grounds, video surveillance, GPS, e-mails, publication of data on the internet, trade unions, health condition, Register of Filing Systems, records.

CONTENTS

About Guidelines

The purpose of the Information Commissioner's guidelines is to provide common practical instructions and procedures for data controllers in a clear and appropriate manner. It seeks to address the most common questions from the area of personal data protection that different data controllers are faced with. With the help of such answers and guidelines, companies and data controllers should accordingly be able to comply with the statutory provisions of the Personal Data Protection Act (Official Gazette of the Republic of Slovenia, No. 94/07 – official consolidated text; hereinafter: ZVOP-1-UPB1).

The legal basis for the Information Commissioner (hereinafter: the Commissioner) to issue the guidelines is provided by Article 49 of the ZVOP-1-UPB1 which stipulates that the Commissioner shall give non-binding opinions, explanations and positions regarding personal data protection, and, further to this, publish these on its website or in other suitable formats, as well as prepare and offer instructions and recommendations regarding personal data protection in individual areas.

See also:

- Commissioner's opinions: http://www.ip-rs.si/index.php?id=383
- Commissioner's brochures: http://www.ip-rs.si/index.php?id=388
- The Commissioner's Guidelines are published on the website: http://www.ip-rs.si/index.php?id=491

Introduction

The legislators preparing the legal frameworks often cannot specifically define their demands because the legal frameworks have to be very specific but at the same time wide enough, and technologically neutral. This can, in practice, lead to different interpretations of the requirements, stipulated by each legal act. ZVOP-1-UPB1 provides a general framework and guidance, supplemented by specific statutes from different areas and case-law. To sustain legal safety, case-law has to be as clear and harmonized as possible.

In the area of employment relationships the need for some guidelines regarding personal data protection appeared. In the case of employment relationships the legal requirements regarding personal data protection are especially important because the employee is the weaker party in relation to the employer, and thus requires a certain degree of protection. That is why this area is covered specifically by other acts as well.

The Commissioner's aim is that the Guidelines become a useful resource for the employees, whose personal data is protected by the Act, and for the employers, who process this data. A harmonized interpretation of the legal requirements of the Act is in the interest of data controllers, as well as in the interest of any subject, who has to establish and maintain the minimum standards for personal data protection, monitored by the state's inspection supervision.

Legal framework for protection of personal data in employment relationships

ZVOP-1-UPB1 provisions are, generally speaking, binding also for personal data controllers from employment relationships. However, because of the specificity of the employment area, the legislator has defined personal data processing in special acts as well. It is necessary to refrain that in the employment relationship the power is unequally distributed, favouring the employer's side; that is why the legislator does not permit the parties to be autonomous. Therefore the employee's personal consent is only admissible exceptionally, in those parts of personal data processing which are not bound to exercising the rights and obligations arising from the employment relationship, or related to the employment relationship of the subject (fox example: distribution of data for new year's employees' children reception). It is also admissible when the employee does not transfer his/her personal data, and therefore cannot suffer any sanctions in the areas of labour legislation.

The employee has to be, firstly treated as an individual with his/her rights as individual, and only secondly as an individual carrying obligations arising from his/her employment relationship. Therefore it is necessary to protect the individual's privacy in his/her work environment; this view is also expressed in the current employment legislation. The fundamental legal act in the field of employment relationships is the Employment Relationship Act (Official Gazette of the Republic of Slovenia, No. 42/02 with changes and additions; hereinafter: ZDR) which contains the following provisions regarding personal data protection:

Article 46
(Protection of the Worker's Personal Data)

(1) Personal data of workers can be gathered, processed, used and provided to third persons only if this Act or other laws stipulate, and if it is necessary in order to exercise the rights and obligations arising from employment relationship or related to employment relationship.

(2) Personal data of workers can only be gathered, processed, used and provided to third persons by the employer or the worker who is specially authorised to do so by the employer.

(3) If the legal basis for gathering personal data of workers does not exist any more, they shall be deleted immediately and no more used.

(4) The provisions of the first three paragraphs shall also apply to personal data of applicants.

Protection of personal data in employment relationships is also defined in the Article 13 of the Labour and Social Security Registers Act (Official Gazette of the Republic of Slovenia, No. 40/06; hereinafter: ZEPDSV), which stipulates the content of employees record:

Article 13
(Records of employees)

The record of employees shall contain for every employee in the employment relationship:
a) the information about the employee:
- *name,*
- *date of birth, if the individual does not posses the unique personal identification number (EMŠO),*
- *place of birth,*
- *the country of birth, if the individual was born outside of the Republic of Slovenia,*
- *unique personal identification number (EMŠO),*
- *tax number,*
- *nationality,*
- *permanent address (street, house number, city, post code, municipality code, country code, country),*
- *temporary address (street, house number, city, post code, municipality code, municipality, country code, country),*
- *education,*
- *whether the employee is disabled,*
- *the category of the disability,*
- *whether the employee has a partial retirement status,*
- *whether the employee is conducting supplementary work for another employer,*
- *the name (and registration number) of the other employer, for whom the employee is conducting supplementary work,*
- *the address of the other employer for whom the employee is conducting supplementary work (street, house number, post code, city);*

b) information about employee's work permit (applicable for foreigners):
- *work permit type,*
- *work permit date of issue,*
- *work permit date of expiry,*

- *work permit number,*
- *the body that issued work permit;*

c) information about the employment contract:
- *the date the employment contract was concluded,*
- *date of commencement of work,*
- *the type of employment contract,*
- *the reasoning behind a temporary employment contract,*
- *the occupation of the employee,*
- *professional skills required for conducting the work and tasks in the employment position for which the contract has been concluded,*
- *title of the position or data on the type of work for which the worker has concluded the employment contract,*
- *stipulation on normal daily or weekly working time,*
- *the organization of working hours,*
- *the place where the work is to be carried out,*
- *whether the employee's employment contract includes a competition clause;*

d) information about the employment contract termination:
- *the date of the employment contract termination,*
- *the manner of the employment contract termination.*
-

Questions regarding personal data protection in individual areas

Types of employees' personal data records

Question: What types of employees' personal data records may the employers process?

Answer: The records from the area of employees' employment and social security the employers may manage are stipulated by Article 13 of the Labour and Social Security Registers Act (ZEPDSV).

Additionally, Article 46 of the Employment Relationship Act (ZDR) provides that the employees' personal data can be gathered, processed, used and provided to third persons only if this Act or other laws stipulate, and if it is necessary in order to exercise the rights and obligations arising from employment relationship or related to employment relationship. This means that the employers can also manage records not provided by statute, however, in that case they have to specifically state or show the purpose for which they require a certain employee's personal data. If the employer does not show that a certain personal data is necessary for the exercise of rights and obligations arising from or related to the employment relationship, he/she has no right to require the employee's personal data.

The Commissioner points out that ZVOP-1-UPB generally draws a distinction between the public and the private sector however the field of employment law is additionally and specifically addressed in particular acts for both sectors. On the basis of Article 9 of ZVOP-1-UPB personal data in the public sector may be processed if the processing of personal data and the personal data being processed are provided by statute. Statute may provide that certain personal data may only be processed on the basis of personal consent of the individual. The employers in the private sector, on the other hand, are subject to the provision of Article 10 of ZVOP-1-UPB, which stipulates that employees' personal data may be processed also on the basis of their personal consent. At this point a warning is necessary: in relation to employment legislation mentioned above (ZEPSDV and ZDR) the personal consent is only valid exceptionally and only for the personal data not bound to exercising the rights and obligations arising from the employment relationship, or in relation to the employment relationship. If the employee does not consent or refuses processing of this kind of personal data, this action should not impact his/her employment relationship in any way.

According to ZVOP-1-UPB an oral or other appropriate kind of individual's consent to data processing is permitted, however the Commissioner recommends that the employers foremost seek to acquire written consent wherever that is possible, and does not present significant cost to them. The reasoning behind this recommendation is the fact that employee's written consent, compared to only oral consent, will undoubtedly be of greater evidence value to the employer in a potential event of a dispute between him/her and the employee.

It is of great importance to point out also the proportionality principle (Article 3 of ZVOP-1-UPB1) which states that personal data that are being processed must be adequate and in their extent appropriate in relation to the purposes for which they are collected and further processed. For example: an employer at the point of employment contract conclusion may not request information about the employees' family or marital status, pregnancy data, family planning data or other information not directly related to the employment relationship (Article 26 of ZDR).

Question: When is the employer obliged to report employees' personal data filing systems to the Commissioner's Register of Filing Systems?

Answer: The Commissioner has to be notified about the existence of all personal data filing systems being processed by the employers. It is not necessary for the employers with less than 50 employees to report the filing systems to the Commissioner's Register, however, this exception is not applicable for data controllers from the public sector, notary, advocates, detectives, executors, private security bodies, private healthcare bodies, public healthcare bodies, and sensitive data controllers, if processing of sensitive data is a part of their registered activity. An employer from the above areas is obliged to report the filing systems to the Commissioner's Filing System Register. A link to the Filing System Register application form can be found on the Commissioner's website (http://www.ip-rs.si/index.php?id=260).

Employment

Question: May a job seeker (hereinafter: the applicant) access his/her test results from the candidate selection procedure?

Answer: The test results, arrived at in the selection procedure on the basis of employer's call for applications, constitute a personal data filing system with entries for each applicant. According to subparagraph 6, Paragraph 1, Article 6 of ZVOP-1-UPB1 the employer is a data controller, and according to Article 30 the applicant has the right to access his/her test results at the employer for whom the tests were taken, in a manner defined by the Article 31 of ZVOP-1-UPB.

Pursuant to Article 30 of ZVOP-1-UPB, the employer as a data controller shall on request of the individual be obliged:

- to enable consultation of the filing system catalogue
- to certify whether data relating to him are being processed or not, and to enable him to consult personal data contained in filing system that relate to him, and to transcribe or copy them
- to supply him an extract of personal data contained in filing system that relate to him
- to provide a list of data recipients to whom personal data were supplied, when, on what basis and for what purpose
- to provide information on the sources on which records contained about the individual in a filing system are based, and on the method of processing
- to provide information on the purpose of processing and the type of personal data being processed, and all necessary explanations in this connection
- to explain technical and logical-technical procedures of decision-making, if the controller is performing automated decision-making through the processing of personal data of an individual

The request from Article 30 of this Act shall be lodged in writing or orally in a record with the data controller. Such request may be lodged once every three months. The data controller must enable the individual to consult, transcribe, copy an obtain data no later than within 15 days, or within 15 days to inform the individual in writing of the reasons why he will not enable consultation, transcription, copying or the issuing of a certificate. If the data controller fails to act in accordance with the above, the request shall be deemed to have been refused. Costs relating to the request and consultation from this Article shall be borne by the data controller.

Question:What happens to the documentation disclosed to the employer in the application procedure by the unselected applicant?

Answer: The documentation containing applicants' personal data, acquired during employer's call for applicants, constitutes a filing system. The employer, managing the filing system, is a data controller under subparagraph 6, Paragraph 1, Article 6 of ZVOP-1-UPB1, and as such he/she is responsible for the applicants' filing system; the processed personal data has to be accurate and kept up to date. The controller is also responsible for appropriate protection of the filing system, for deleting, destroying, blocking or anonymizing of personal data upon the completion of the purpose for which the data has been processed.

Under Article 21 of ZVOP-1-UPB1 personal data may only be stored by the data controllers (the employers who called for applicants), for as long as necessary to achieve the purpose for which it was collected or further processed. On completion of the purpose of processing, personal data shall be erased, destroyed, blocked or anonymised, unless it is defined as archive material pursuant to the statute governing archive materials and archives, or unless a statute otherwise provides for an individual type of personal data.

Paragraph 3, Article 46 of ZDR which applies to applicants' personal data as well, also stipulates that that if the legal basis for gathering personal data of workers does not exist any more, it shall be deleted immediately and no more used. On completion of the selection procedure the employer does not require the applicants' personal data in order to exercise the rights and obligations arising from employment relationship or related to employment relationship. Therefore the employer has no legal basis for further processing of personal data and, to comply with Article 46 of ZDR, the personal data has to be destroyed.

The rights of the non-selected applicants are defined in detail in the Article 28 of ZDR, under which the employer has to notify in writing the applicant who was not selected of the fact that he was not selected within eight days after concluding the employment contract. The employer must return to the applicant who was not selected at his request all the documents submitted as proof of fulfilment of required conditions for carrying out work.

It follows from the above that every non-selected applicant has the right to request all the documents submitted as proof of fulfilment of required conditions for carrying out work. If the not-selected applicant does not request the documents, the employer is obliged to destroy it.

Question: May the employer, at the point of employment contract conclusion, copy employee's personal identification document?

Answer: Crucial for answering this question is the fact that the employer may only collect personal data included in the employee's personal identification document and at the same time stipulated by the Article 13 of the ZEPDSV (for instance unique personal identification number, permanent address…). The employer may check the employee's personal document to verify the accuracy of information before entering it into the filing system. However, he/she has no legal ground for copying the personal identification document.

Comparing the data stipulated by the Article 13 of the ZEPDSV and the data that can be found in the personal identification document, we see that a personal photography is not among the data the employer may collect. A personal identification document usually includes photography - a personal data that the employer is not entitled to collect - hence the employer has no legal basis for requesting a copy of a personal identification document. The primary function of personal identification documents is identification of the individual hence the employer can transcribe the information from the document, but may not copy it.

It is important to keep in mind Article 46 of ZDR as well, under which workers' personal data can be processed even if not stipulated by statute, if it is necessary in order to exercise the rights and obligations arising from employment relationship or related to employment relationship. This means that the employer has to state or show specifically why an employee's personal information, not included in the ZEPDSV or another Act, is necessary. If the employer does not show that this data is necessary in order to exercise the rights and obligations arising from employment relationship or related to employment relationship, he/she may not request a copy of a personal identification document that includes the above data.

Question: May the employer request a Police Clearance Certificate from an employee with a valid employment contract?

Answer: The employer is in recruitment of new employees, with respect of the legally determined limits, free to set the conditions the potential employees have to fulfil. With this in mind, the employer has the freedom to request a Police Clearance Certificate for certain work positions, however under Article 23 of ZDR this condition has to be announced in advance in the public advertisement of vacancy.

The Commissioner emphasises that in relation to Police Clearance Certificate requests the employer is limited by the conditions specified in the Article 46 of ZDR: the employer may request the Certificate, if stipulated so by ZDR or another Act, and if it is necessary in order to exercise the rights and obligations arising from employment relationship or related to employment relationship. If collection of sensitive data, in this case Police Clearance Certificates, is necessary in order to exercise the rights and obligations arising from employment relationship or related to employment relationship, the Commissioner emphasises that the decisions on the necessity of data processing have to be case-specific for each individual. Crucial in deciding is the proportionality principle which stipulates that the personal data that is being processed (which includes collection as well) must be adequate and in their extent appropriate in relation to the purposes for which it is processed.

The basis for Police Clearance Certificates are criminal records, hence this is sensitive data. The Commissioner warns that collecting such data in the public sector requires legal basis or if the law so stipulates legal basis and an individual's explicit personal consent. The Commissioner also reiterates that under ZVOP-1-UPB1 such data requires stricter protection. Article 14 of ZVOP-1-UPB1 stipulates that the employers from public and private sector - processing sensitive data - have to specifically define the scope of this data and protect it in a way that prevents unauthorised access to it. Where telecommunications transfer of sensitive data is used, the data is appropriately protected, if it is transferred using cryptographic methods or electronic signature in such a way that the data during transfer cannot be read or recognized.

Information about trade union membership, and the function of trade unions in processing of employees' personal data

Question: Is the employer allowed to collect data about employee's trade union membership?

Answer: According to Article 13 of ZVOP-1-UPB1, sensitive personal data, which also include information about trade union membership (subparagraph 19, Article 6) may only be processed in eight individual cases. It is necessary to stress that sensitive data processing in the public sector requires explicit personal consent (normally written) and also explicit legal basis stipulated by a statute governing a certain area.

Firstly, collecting data about union membership is made possible by the subparagraph 1, Article 13 of ZVOP-1-UPB1, which stipulates that the employer in the public sector may only process data about trade union membership, if the individual has provided explicit consent which should be defined in the sector-specific law. Such consent should as a rule be written.

It is also possible to collect this data under subparagraph 2, Article 13 of ZVOP-1-UPB1, which says that sensitive data may be processed, if processing is necessary in order to fulfil the obligations and special rights of a data controller in the area of employment, in accordance with statute which also provides appropriate guarantees for the rights of the individual. An example would be the clearance of trade union membership fee, which is not possible without the information about the names of trade unions the individual employees are members of. A direct legal basis for processing is also Paragraph 3, Article 210 of ZDR which says that upon a request of the trade union and in compliance with the regulation of the trade union the worker is a member of, the employer shall ensure the technical execution of settlement and payment of a trade union membership fee for the worker concerned. Therefore, if the trade union members wish not to reveal their membership to the employers, they will have to pay the membership fee directly to the trade union and not through the employer.

Question: May the employer disclose the information about employees' wages to the trade union?

Answer: Under Article 207 of ZDR an employer shall be obliged to grant the trade union access to information as may be necessary for the exercise of trade union activities.

The Commissioner's opinion is that the provision of ZDR gives trade unions appropriate and satisfactory legal basis for admissible processing of personal data they need for the exercise of trade union activities. The trade unions can only perform their activities (negotiations, irregularities in employer's activities), if they have access to personal information. Following from the above the employer does not require employee's personal consent for disclosing information about the wages to the trade union, hence the disclosure does not constitute a breach of ZVOP-1-UPB1. However, trade unions have to act in accordance with proportionality principle and only request or access data necessary and suitable for exercising specific union activities (thus the trade union does not have the right to access information about employee's credits or alimonies, etc.). This means that the trade union has to explain every request and show that it has legal grounds for it, so that the employer will be able to supply the right documentation and to ensure traceability of granted access stipulated by subparagraph 5, Paragraph 1, Article 24 and subparagraph 4, Paragraph 1, Article 30 of ZVOP-1-UPB1.
Question: What is the role of trade unions in implementation of video surveillance?

Answer: Under Paragraph 5, Article 77 of ZVOP-1-UPB1 the employer is obliged to consult with the representative trade union, prior to the introduction of video surveillance. The employer is therefore obliged to carry out a consultation with the representative trade union; however, this does not mean that he/she is bound by the trade union's opinion. It is sufficient for the employer to notify the representative trade union about the proposed implementation of video surveillance and call for its opinion on the matter. The employer is later not bound to this opinion, nor have the representative trade unions the obligation to express its opinion. Considering the above, the Commissioner advises the employers to hold a consultation with the representative trade union and request for it to deliver an opinion on the introduction of video surveillance in a reasonable time period (the Act itself does not quantify the time period in relation to this provision). If the trade union does not react upon this request, as already mentioned, this does not represent an obstacle for employers to implement video surveillance.

Processing of healthcare personal data

Question: Is the employer entitled to know about the employee's sick leave and movement regime in the context of sick leave?

Answer: The employer is not entitled to know about the diagnosis of the sick employee but he/she is entitled to be notified of the employee's sick leave and movement regime (and not the treatment regime) in the context of sick leave to verify the justification of absence from work. The issued confirmation of justified absence from work should thus never include a diagnosis or specific description of the disease or injury, but only the information necessary and admissible for the employer and the health insurance company (whether the disease or injury is professional, whether it occurred outside of work activities, whether it is the type of absence where the employee is entitled to sick pay starting with the first day of absence). To the best of the Commissioner's knowledge this indeed is a standard practice – the confirmations are usually given on a standard form, which is widely used by all the doctors.

The doctor may notify the employer, in a way that shall not permit unauthorised access to personal information, whether the employee's absence from work because of a disease or injury (that has occurred outside of or during work activities) is justified, and how long this absence will be. The Commissioner hereby warns that it is not recommended to transmit this data over the telephone, because in this case the identity of the recipient cannot be verified. The data controller (in this case the doctor) has to know or verify whether he has given the information to the right person. It follows from the above that the employer may collect the certificates of justified absence from work (originals or photocopies) according to Article 46 of ZDR. This information is already a part of the personal data filing system therefore it is not necessary for the employer to report it as a special filing system. However, data about justified absence from work has to be mentioned in the filing system catalogue as one of the categories of data the employer is collecting.

A confirmation of the employer's right to collect this data can be found in the Health Care and Health Insurance Act (Official Gazette, No. 9/92, with changes and additions; hereinafter: ZZVZZ). Under this Act the employer is obliged to finance absence from work as a result of sickness or injury for a limited period of time. At the end of the month the employer receives a confirmation of sickness or, if the absence is longer than 30 days, a decision issued by the Health Insurance Institute of Slovenia, where the period of sickness together with appropriate instruction is stated. The employer usually receives this decision before termination of sick leave. The employer will therefore be notified about the employee's sick leave, however with delay, which conflicts his right to control. Thus the employer is entitled to have the information about the employee's general practitioner (GP) and movement regime during justified absence or sick leave earlier.

Question: Who may perform supervision of sick leave and what may be the scope of this supervision?

Answer: The employer has, according to Article 111 of ZDR, the power to extraordinarily terminate the worker's employment contract, if the worker during the period of being absent from work because of disease or injury, fails to respect the instructions of the competent doctor and/or of the competent medical commission, or if he in this period carries out gainful work or leaves his residence without the approval by the competent doctor and/or by the competent medical commission. It follows from the provisions of Article 46 and Article 111 of ZDR that supervision of sick leave is actually necessary in some cases in order to exercise the rights and obligations arising from employment relationship. In this case the supervision of sick leave is regarded as personal data processing due to the collection, dissemination and use of data related to the sick leave situation. Therefore the supervision of sick leave and related personal data is admissible under ZVOP-1-UPB1, if it is implemented with due respect of the principle of proportionality from Article 3 of ZVOP-1-UPB1.

The supervision of sick leave and related personal data processing may be performed by the employer himself or according to Article 11 of ZVOP-1-UPB1 by a contracted third party. The employer has to clearly state or show why processing of personal data is necessary. If the supervision is performed by a contracted party, on a basis of a written contract, the contractor may only be a person that is registered to perform supervision and security activities, and has to perform their activities pursuant to Detective Activities Act (Official Gazette, No. 96/07; ZDD-UPB-3). The Act defines the conditions for performing detective activity, the rights and obligations of detectives in terms of personal data acquiring, the appropriate level of detective's professional training and the inspection over the exercise of the Act's provisions. The inspection also provides for appropriate standards in terms of personal data processing. The employer may perform the control himself/herself, however with other means of supervision (home visits…).

Question: Which information about an employee's disability is the employer entitled to acquire?

Answer: The employee is obliged to notify the employer about the disability category and the limitations that emerge as a consequence of the disability (for instance ban on heavy lifting, ban on height works, part time work etc.). The employer needs to get this information in order to assess whether he/she has a suitable work position, whether he/she can adapt the position to the abilities and needs of a disabled person, whether the disabled person needs to be provided with professional and technical support (informing, counselling and qualifying, personal assistance, escort at work, assessment of work efficiency). The employee proves the above with a document issued by a competent body which states the category of disability and explains what the employee is capable of. The document is

issued by the Pension and Disability Insurance Institute of the Republic of Slovenia who is under Paragraph 1, Article 179 of ZUP obliged to issue a confirmation about the facts in its records. This confirmation may also be attached to work applications because it is regarded as an official confirmation. Only when the selection process is near the end or when the employment contract is being concluded, the candidate has to supply to the employer additional documentation about the disability. The documentation has to clearly state the work abilities of an individual for the employer to be properly notified about the employees' condition.

The Commissioner emphasises that the rules of personal data protection are set also for general practitioners (GP) in the General Practitioner Services Act (Official Gazette, No. 98/99 with changes and additions; hereinafter: ZZdrS-UPB3). Article 51 stipulates that the practitioner has to protect, as a professional secret, the data on patient's health condition, and the data about the causes, context, and consequences of the condition. Article 52 stipulates that this data is not to be transferred to other people or public (thus even the employer) and not to be published in a way that would enable identification of the individual. This means that a general practitioner shall not communicate any information about employee's health condition to the employer.

Question: May the employer request for the name of the employee's general practitioner and the address of the outpatient's department?

Answer: In certain cases the information about the employee's general practitioner and the address of the outpatient's department can be important in order to exercise the rights and obligations arising from employment relationship. This follows from the provisions of Article 46 of ZDR and Article 111 of ZDR which stipulate that the employer may extraordinarily terminate the worker's employment contract, if the worker during the period of being absent from work because of disease or injury, fails to respect the instructions of the competent doctor and/or of the competent medical commission, or if he in this period carries out gainful work or leaves his residence without the approval by the competent doctor and/or by the competent medical commission.

Because of the necessary supervision of the sick leave, which also means processing of personal data related to sick leave, the information about employee's general practitioner and the address of the outpatient's department may be necessary for control over the exercise of rights and obligations arising from employment relationship. The Commissioner hereby warns that the principle of proportionality from the Article 3 of ZVOP-1-UPB1 has to be strictly pursued in such context. The employer may only acquire the information about the general practitioner and the address of the outpatient's department and not other data as well.

Publication of employees' personal data

Question: According to ZVOP-1-UPB1, may the employer publish the employee's e-mail address on a website?

Answer: Crucial in this case is the provision of Paragraph 2, Article 106 of ZVOP-1-UPB1 which stipulates that data controllers may supply to the public and publish the personal name, title or function, official telephone number and official electronic mail address of the head and those employees whose work is important for operations with clients or users of services, until the entry into force of a special statute regulating this issue.

The provision refers to the public as well as private sector employers. It means that the employers can freely transmit or publish the data (over the internet for instance) regardless of the lack of other legal grounds in another act, and therefore do not require a public employee's personal consent. This provision is an independent legal ground which enables the employer to freely decide on matters of data publishing. The Commissioner hereby points out that the employer is still limited: published personal data may only consist of a name, title, work phone number and work e-mail address of the employees. At the same time the employer may only publish information about the head and those employees whose work is important for operations with clients or users of services.

Publication of employee's e-mails on the websites with the purpose of simpler communication with clients is therefore in accordance with ZVOP-1-UPB1 if those are the e-mails of the head and those employees whose work is important for operations with clients or users of services.

Question: May the employer publish (for instance on the internet or intranet) employee's photography without his/her consent?

Answer: According to Article 46 of ZDR personal data may be processed even without explicit legal ground. Based on this provision the employer may publish an employee's photography if it is necessary in order to exercise the rights and obligations arising from employment relationship or related to employment relationship (for instance for fashion models). The employer has to specifically state or show why he/she requires the photography to be published. If the employer shows that the publication of employee's photography is necessary in order to exercise the rights and obligations arising from employment relationship or related to employment relationship, he/she does not require employee's consent, because he/she has legal grounds in the Article 46 of ZDR.

The Commissioner however emphasises that the employer has to consider the principle of proportionality (Article 3 of ZVOP-1-UPB1) when publishing photographies: the Act stipulates that personal data that are being processed must be adequate and in their extent appropriate in relation to the purposes for which they are published.

Video and audio surveillance and surveillance with GPS (global positioning system) technology

Question: Under which conditions is video surveillance permitted within the workplace?

Answer: The Commissioner emphasises that video surveillance as stipulated in the ZVOP-1-UPB1 only occurs when a filing system of personal data (in this case a collection of video files) originates during video surveillance. The Commissioner is only competent to consider potential breaches when the personal information is in the filing system, and it is being processed.

The general provisions regarding video surveillance are stated in the Article 74 of ZVOP-1-UPB1: a public or private sector person that conducts video surveillance must publish a notice to that effect. Such notice must be visible and plainly made public in a manner that

enables individuals to acquaint themselves with its implementation at the latest when the video surveillance of them begins. According to Paragraph 3, Article 74 the notice must contain the following information:

1. that video surveillance is taking place
2. the title of the person in the public or private sector implementing it
3. a telephone number to obtain information as to where and for which period recordings from the video surveillance system are stored

In the context of video surveillance within work area the Commissioner draws attention to Paragraph 1, Article 77 of ZVOP-1-UPB1 which stipulates that video surveillance within work areas may only be implemented in exceptional cases when necessarily required for the safety of people or property or to protect secret data and business secrets, and where such purpose cannot be achieved by less invasive means. According to Paragraph 2 video surveillance may only be implemented for those parts of areas where the interests from the previous paragraph must be protected. Paragraph 3 stipulates that video surveillance shall be prohibited in work areas outside of the workplace, particularly in changing rooms, lifts and sanitary areas. According to Paragraph 4 employees must be informed in advance in writing prior to the commencement of implementation of video surveillance and Paragraph 5 stipulates that prior to the introduction of video surveillance in a person of the public or private sector, the employer shall be obliged to consult the representative trade union at the employer.

The Commissioner hereby summarises the conditions that have to be fulfilled for the employer to implement video surveillance inside workplaces:

- video surveillance has to be necessarily required for the safety of people or property or to protect secret data and business secrets;
- such purpose cannot be achieved by less invasive means;
- video surveillance may only be implemented for those parts of areas where the interests from the Paragraph 1 of ZVOP-1-UPB1 must be protected;
- employees must be informed in advance in writing prior to the commencement of implementation of video surveillance;
- prior to the introduction of video surveillance the employer shall be obliged to consult the representative trade union at the employer;
- video surveillance shall be prohibited in work areas outside of the workplace, particularly in changing rooms, lifts and sanitary areas.

The Commissioner also draws attention to the proportionality principle written in the Article 3 of ZVOP-1-UPB1, according to which it shall be considered in each specific case whether there are less invasive means available whereby the work areas with employees would be excluded from the area recorded by the video surveillance cameras. European Court of Human Rights highlighted the right to privacy in workplace in the Halford vs. United Kingdom case (25. 6. 1997, Reports 1997-111) where it stated, that an individual has a reasonable expectation of privacy, even in the workplace. The question of privacy protection in the employer-employee relationship has to be always considered on a case-to-case basis because a collision of multiple interests occurs in this situation. On the one hand the employer has the right to govern his/her resources (thus also the right to supervise it), and on the other hand the employee has a legitimate right to expect a certain degree of privacy, partial independence and confidentiality in the workplace (further reading in The Constitution of the Republic of Slovenia, With Comments, ed. Šturm, Fakulteta za podiplomske državne in evropske študije, 2002, from p. 401 on).

Based on the above it follows that in the process of employer's governing of his/her resources the employee's right to privacy should not be overlooked. Protection of employer's resources cannot be executed in a way that would breach the individual's right to privacy in the workplace. On the other hand, however, exaggerated protection of privacy cannot lead to a position where the employer's right to protection of resources would have been dismissed. In the end, both are constitutional rights (Article 35 and further of the Constitution of RS – the right to privacy; Article 67 of the Constitution of RS – property).

Additional information on video surveillance can be found on the Commissioner's website:
http://www.ip-rs.si/varstvo-osebnih-podatkov/informacijske-tehnologije-in-osebni-podatki/videonadzor/

Question: Under which conditions is video surveillance of access to official office premises and business permitted?

Answer: In accordance with Article 75 of ZVOP-1-UPB implementation of video surveillance of access to official office premises or business premises is permitted if it is necessary for security of people or property, for ensuring supervision of entering to or exiting from their official or business premises, or where due to the nature of the work there exists a potential threat to employees. The decision shall be taken by the competent functionary, head, director or other competent or authorised individual of the person in the public sector or person in the private sector. The written decision must explain the reasons for the introduction of video surveillance. The introduction of video surveillance may also be laid down by statute or a regulation issued pursuant thereto.

All employees of the person in the public or private sector working in the premises under surveillance must be informed in writing of the implementation of video surveillance.

The filing system under this Article shall contain a recording of the individual (an image or sound), and the date and time of entry to and exit from the premises, it may also contain

the personal name of the recorded individual, the address of his permanent or temporary residence, employment, the number and data on the type of his personal document, and the reason for entry, if the personal data listed are collected in addition to or through the recording of the video surveillance system.

Personal data from the previous paragraph may be stored for a maximum of one year from their creation, and shall then be erased, unless otherwise provided for by statute.

Question: Is the employer permitted to establish a record on employees using GPS technology?

Answer: The interpretation of employee's right to privacy in the workplace is developing, which has been affirmed by the European Court of Human Rights in the Halford vs United Kingdom and Copland vs United Kingdom cases. The employer has no right to access employees' e-mails, control the use of work phone when the employee has the right to use it for private purposes as well, and has no right to track the movement of work vehicles with GPS technology, when the vehicles are also used for private purposes, etc. Case-law indicates that the employer cannot justify the control over privacy (especially communication privacy, i.e. confidentiality of all the forms of communication – post, telephone, e-mail) with the fact that the work means (the vehicle, telephone) are his/her property and hence he/she has the right to manage them.

GPS technology is a satellite navigation system used for determining the exact position and time anywhere in the world. Aside from personal use, GPS technology brings benefits when used commercially, for instance in vehicle fleets management, because it reduces the cost of supply and logistics chain optimization and subsequently enhances productivity.

Each technology is by itself neutral however its application (manner of use) can present a threat to personal data protection. The Commissioner's opinion is that the employer may have legitimate grounds for implementation of vehicle fleet tracking but he/she has to consider the use of such technology with reference to personal data protection. The employees have a legitimate right to a reasonable expectation of privacy within the work area, hence in the work vehicle, especially if the vehicle may be used for personal purposes outside of working hours.

The Commissioner draws attention to the recent decision of the European Court of Human Rights in the Copland vs. United Kingdom case. The Court extended the employee's right to privacy by adjudicating that the employer's breach of privacy was unjustified. Crucial for the decision was the fact that the employee had not been informed about when, and in what cases the employer may control the e-mails.

The same principle must be applied in the case of GPS technology surveillance. The employee has to be informed in advance about when, and in what cases the employer may control the vehicle. Usually the use of work vehicles is defined specifically in internal acts of organizations (i.e. rules about vehicle fleet use). The Commissioner believes that use of any kind of vehicle tracking technology, including GPS, has to be defined specifically in an act like that. All the employees, or at least the ones who use the vehicles, have to be informed about the terms of use. The employer has to respect the principles of personal data protection and safeguard the employee's right to privacy when implementing vehicle tracking technology. He/she has to clearly inform the employees about the ways the technology may be used, the ways it works, the purpose of its implementation, and the situations in which the acquired data may be used. Additionally, it has to be clear that the data may only be used for purposes and in situations, clearly defined in advance.

There is a chance that when implementing GPS technology, a filing system, protected by the provisions of ZVOP-1-UPB1 and thus in the competence of the Commissioner, will emerge. A question of when, under which conditions, and for what purpose the employer may establish this kind of a filing system, hereby emerges as well.

ZVOP-1-UPB is an umbrella act in the area of personal data protection in the Republic of Slovenia. It defines the scope of protected data and the principles of data protection, and thus enables legal protection of a constitutional right to privacy. Because of the specificity of employment relationships the legislator does not predict autonomy of the parties but rather permits only such processing of personal data as stipulated by statute. The filing system based on the use of GPS technology is not among the records defined by the ZEPDSV. Therefore, it is necessary to consider Article 46 of ZDR, which stipulates that the employer has to show that personal data processing is necessary in order to exercise the rights and obligations arising from employment relationship. If the employer does not show that the personal data is necessary in order to exercise the rights and obligations arising from employment relationship, he/she may not request the data from the employee or gather this data from other persons.

When the use of GPS technology is necessary, this can only be judged on a case-to-case basis. Different elements have to be considered when making the decision. Most of all, it is necessary to consider the purpose of the employer wishing to implement such technology. The purpose has to be earnest, and justified with enough evidence. Arguments about the necessity of GPS implementation at a flat rate shall not be enough. The employer has to determine whether he/she could have reached the same purpose satisfactorily enough with less invasive means for privacy, freedom of movement, and employee's dignity. The Commissioner doubts that implementation of GPS is necessary in a large number of cases. When implementing GPS technology the employer has to pay attention to technical aspect as well. Pursuant to ZVOP-1-UPB1 the following issues have to be considered: who has access to this data, is the data sufficiently protected, in what form the data is stored etc. When implementing GPS technology one has to consider all the aspects of such technology.

The Commissioner believes that the technology is not suitable for all types of supervision of employees, for instance for the record of working hours. A data controller wishing to implement GPS as a means for working hours recording, would have to prove that for the purposes he/she pursues, such measures are necessary and that it would be impossible to achieve the purpose in a way less intrusive in terms of privacy, freedom of movement, and employees' dignity. Data controllers should not use this kind of technology just for the sake of simplicity or because they wish to prevent abuse of the vehicle fleet. In this case a proof would be necessary that the scope of the abuse is such that it represents a threat to the organization. Mere listing of reasons without a suitable substantiation supported by proof shall not be enough.

This means that the employer has to specifically state or show why he/she needs personal data acquired by the use of GPS tracking devices. If the employer does not show that he/she requires this personal data in order to exercise the rights and obligations arising from employment relationship, he/she may not use a GPS tracking device in a way where a record showing the exact position of an individual in a given time frame emerges.

If the employer shows that the required personal data is necessary in order to exercise the rights and obligations arising from employment relationship, The Commissioner reiterates that it is his/her duty to inform the employees about such surveillance. The employer has to state in advance when, and in which cases such surveillance may occur, and additionally, this has to be defined in an appropriate internal organizational act. The use of technology, its activity and the purpose of implementation have to be clearly defined together with the possible situations when the acquired data may further be used.

Question: Is the employer allowed to record telephone conversations between employees, and later reproduce them?

Answer: The Electronic Communications Act (Official Gazette RS, No. 13/07; hereinafter: ZEKom) stipulates confidentiality of electronic communications in Paragraph 6, Article 103 where it provides that subscribers or users may record communications, but they shall be obliged to inform the sender or recipient of the communication thereof or adjust the operation of the recording device such that the sender or recipient of the communication is informed of its operation (e.g. answering machine). Pursuant to this provision and on the basis of ZVOP-1-UPB1 provisions it is possible to logically explain the basis for recording with the fact that the employee – the user of electronic communications – is informed about the recording at the moment the connection is established. It is necessary also to note the provision of Article 19 of ZVOP-1-UPB1 which in Paragraph 1 stipulates, that if personal data are being collected directly from the individual to whom they relate, the data controller or his representative must inform the individual about the purpose of personal data processing. If the employee is not undoubtedly informed about the recording, the data controller (in this case the employer) is most likely breaching Article 19 of ZVOP-1-UPB1, as well as Article 103 of ZEKom.

Reproduction of the acquired records is not possible if the employee has only given personal consent for recording and not for reproduction as well. If the employer does not have personal consent for reproduction, he/she may only reproduce recordings if stipulated by statute (and not only by a decree for instance).

It is also necessary to consider Article 46 of ZDR pursuant to which recording without consent indicates a breach of ZDR. The employee has the right to privacy in the workplace, which has been established by the European Court of Human Rights in the Halford vs. United Kingdom, and Slovenian constitution law theory (further reading in The Constitution of the Republic of Slovenia, ed. Šturm, Fakulteta za podiplomske državne in evropske študije, 2002, form p. 401 on). European Court of Human Rights reiterated the importance of the right to privacy in April 2007, in the Copland vs. United Kingdom case. The Court adjudicated that the employer's breach of privacy was unjustified and extended the employee's right to privacy. The crucial element of the adjudication was the fact that the employee had not been informed about when, and in what cases the employer may control the e-mails.

It is important also to point out the Article 21 of ZVOP-1-UPB1 which defines the duration of personal data storage. Personal data may only be stored for as long as necessary to achieve the purpose for which they were collected or further processed. On completion of the purpose of processing, personal data shall be erased, destroyed, blocked or anonymised, unless a statute otherwise provides for an individual type of personal data.

An exception from the above provision can be found in the Paragraph 7, Article 103 of ZEKom, according to which recording of communications and the associated traffic data shall be permitted within the framework of lawful business practice with the objective of securing evidence of market transactions or any other business communications, or within organisations receiving emergency calls, for their registration, identification and resolution.

However, the Commissioner warns that in accordance with the proportionality principle in Article 3 of ZVOP-1-UPB1 the exceptions have to be interpreted narrowly and in the interest of employee's privacy. That is why we advise the employers to thoroughly consider all the legal requirements prior to any implementation of telephone (or other communication) conversation recording, and most importantly, to widely inform the employees prior to implementation.

The Commissioner warns that recordings which do not pursue the provisions of ZEKom and ZVOP-1-UPB1 are illegal and as such subject to criminal law statutes and other sanctions for misdemeanour provided by specific Acts.

There are no legal grounds for implementation of telephone conversation recordings by the employer with the purpose of supervision of the employee's execution of work obligations. Any such attempt could be regarded as a criminal offence, in the light of Article 148 of the Penal Code of the Republic of Slovenia (Official Gazette RS, No. 95/04, official consolidated text; hereinafter: KZ), which defines unjustified wiretapping and sound recording as criminal offence.

The use of biometrics

Question: Is it admissible to verify employee's presence at work with biometric technology?

Answer: Verification of employee's presence at work, using biometric means is thoroughly explained in the Commissioner's guidelines which can be found at: http://www.ip-rs.si/index.php?id=491

Electronic communications and protection of employees' personal data

Question: To what extent is the employee's electronic communication privacy protected in the work area?

Answer: The employee's electronic communication privacy is thoroughly explained in the Commissioner's guidelines which can be found at:http://www.ip-rs.si/index.php?id=491

Conclusion

Protection of employee's personal information should enjoy great importance in the exercise of rights and obligations the employer has as a stronger party in employment relationships. The employer has to be aware that this position gives him/her the power to severely influence the employee's constitutional right to privacy. That is why he/she has to be careful, deliberate, and act in accordance with the statutes governing this area. The Commissioner recommends that the employer clears the specific questions regarding personal data protection in advance in internal acts, and informs the employees about this. Most importantly, the employer should try to comply with the legal requirements on privacy and, whenever possible, do this in discussion with the employees. This kind of treatment will surely lead to a trustful relationship between the parties in the employment relationship and subsequently enhance work effectiveness.

The legislator has taken care of the legal protection of the employee as the weaker party in the employment relationship. The employee has the possibility of filing a complaint to the Commissioner, if he/she believes the employer has breached the legal provisions regarding personal data protection.