Guidelines on video surveillance

A manual that explains the rules on the introduction of video surveillance, and calls attention to the most frequest violations of law in its implementation.

INFORMATION COMMISSIONER

Contents

3 About Information Commissioner's guidelines
3 Introduction
4 General conditions for implementation of video surveillance
5 *Video surveillance of access to official office premises and business premises*
6 Specific questions on data protection
8 Security of video surveillance system
9 *Video surveillance, generally*
11 Video surveillance of workplace
11 *General information about privacy and personal data protection in the workplace*
12 *Answers to specific questions*
15 Video surveillance and apartment buildings

About the guidelines

These guidelines have been prepared by the Information Commissioner (IC) as a practical and useful guide to be used by data controllers. The guidelines are written in a simple and accessible languege, in a form of frequently asked questions. Through the answers provided the data controllers will learn how to handle personal data in an appropriate manner and compliant with the requirements of the Personal Data Protection Act (Official Gazette RS, No. 94/07 – official consolidated text; hereinafter: ZVOP-1).

The legal basis for publishing this text derives from Art. 49 of ZVOP-1, under which the Information Commissioner may prepare and issue non-binding instructions and recommendations regarding protection of personal data in individual fields and publicise the information on its website, or communicate such information in some other manner.

See also (click):
Opinions of the IC

Brochures of the IC

The Guidelines

Introduction

In setting legal frameworks the legislator cannot foresee all the details of the legal requirements. The legal framework has to be very concrete, but the same time wide enough and foremost technologically neutral, which may, in practice, bring different interpretations regarding the requirements of a legal document. The Personal Data Protection Act thus sets an overall framework and policies which are then accompanied by sectoral legislation and practices. Because of legal certainty the legislation should be as far as possible uniform and clear.

In practice the law may not always be clear regarding the scope and admissibility of video surveillance. That is why practical questions pertaining to implementation of video surveillance arise.

Video surveillance is the field where the Information Commissioner most frequently encounters violations of the law and these guidelines should be of assistance to those who already perform video surveillance and have questions regarding compliance with the law, as well as to those only thinking of implementing video surveillance.

The legal framework for video surveillance set in the Personal Data Protection Act (ZVOP-1)

General conditions for implementation of video surveillance (Article 74)

According to Article 74 of ZVOP-1 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 about its implementation at the latest when the video surveillance of them begins. 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.

The video surveillance system must be protected against access by unauthorised persons.

The public or private person conducting video surveillance must, according to Articles 24 and 25 of ZVOP-1 define technical and logical-technical procedures and measures to protect personal data in the internal acts, as well as to provide for security of data in the manner prescribed by Article 24 of ZVOP-1.

The persons responsible for video surveillance filing systems and the persons who, due to the nature of their work, process the data also have to be defined.

According to Article 24 it is necessary to establish records that enable subsequent determination of when individual video surveillance data were used or otherwise processed, and who did so, for the period covered by statutory protection of the rights of an individual due to unauthorised supply or processing of personal data.

Article 26 of ZVOP-1 also states that a filing system catalogue has to be established for video surveillance records. The data from the filing system catalogue have to be supplied to the national supervisory body for data protection (Article 27 of ZVOP-1). More information is available on the Information Commissioner's website.

Exceptions

According to Para 4 Article 7 of ZVOP-1, data controllers with fewer than 50 employees are not required to fulfil the obligations on the internal act on data security, on the establishment of a filing system catalogue and supply of the data from the catalogue to the register handled by the Information Commissioner. However, according to Para 5 Article 7 of ZVOP-1 the following are not exempt from these obligations:

- data controllers in the public sector,
- notaries public,
- attorneys,
- detectives,
- bailiffs,
- private security providers,
- private healthcare workers,
- healthcare providers, and
- data controllers that keep filings systems containing sensitive personal data and processing of sensitive personal data is a part of their registered activity.

Video surveillance of access to official office premises and business premises (Article 75 of ZVOP-1)

The public and private sector may, according to Article 75 of ZVOP-1, implement video surveillance of access to their official office premises or business premises only if necessary for the 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 must be taken by the competent functionary, head, director or other competent or authorised individual of the person in the public sector or the 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.

Video surveillance may only be implemented in a manner that does not show recordings of the interior of residential buildings that do not affect entrance to their premises, or recordings of entrances to apartments.

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 containing data on video surveillance of access to business or official premises may contain recordings 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. The data on video surveillance may be stored for a maximum of one year from their creation, and shall then be erased, unless otherwise provided for by the law.

Specific questions on data protection

Question: Can a notice on the implementation of video surveillance be published in the media?

Answer: The notice may be published in the media however this does not meet the legal requirements.

Para 2 Article 74 makes it clear that the notice on video surveillance must be made public in a manner that enables individuals to acquaint themselves about its implementation at the latest when the video surveillance of them begins. This means that every individual entering the area of video surveillance has to be notified. Notices in the media cannot be regarded as an assurance that all individuals entering the area of video surveillance are familiar with it (a classic example – an individual who was abroad at the time of publication in the media cannot know that a given entity implemented video surveillance).

Question: Must there be a notice, even if we have installed "blind" cameras (that do not record)?

Answer: No, but it is recommended, as this creates additional protection impact.

As defined in the introductory articles (see in particular points 3 and 5 of Article 6) ZVOP-1 protects foremost the data contained in filing systems. Blind cameras do not record, i.e. no personal data filing system is established. That is why blind cameras cannot be regarded as video surveillance in terms of ZVOP-1.

Question: Is it necessary for all three elements from Para 3 Article 74 to be included in the notice?

Answer: Yes.

ZVOP-1 even expressly sanctions the data controllers who (even if negligently) leave out any of the information - see point 2 Para 1 Article 95 of ZVOP-1. The penalties may be very high, so data controllers are advised to be particularly careful in preparation of notices on video surveillance. Special attention should be paid in cases where video surveillance is entrusted to a contractor (for example to a security company) – a data processor, who performs video surveillance on behalf of the data controller. In this case it is wrong for the processors to publish a notice, saying that they are

performing video surveillance, as in fact they are doing so on behalf of their client. That is why the notice should include the name of the data controller, and not the name of the data processor.

Question: Is it necessary to publish a notice in apartment buildings although all residents are aware of video surveillance?

Answer: Yes (Because of the guests who come to visit. Video surveillance is an intrusion into their privacy as well.).

Article 74 does not offer any exemptions for data controllers wishing not to provide the notice. Even if all the residents of the apartment building are familiar with video surveillance, it is still necessary to notify the visitors of the building who are not familiar with it.

Question: Is it necessary to publish a notice when performing video surveillance in public areas?

Answer: The notice is essential when individuals may be identified from the recorded material, and preferable in all other cases (for example also in panoramic images where individuals may not be identified).

Taking into account points 1 and 2 of the Para 1 Article 6, ZVOP-1 defines personal information as any information pertaining to an identified or identifiable natural person. Thus if an individual cannot be identified from the image in any event (the face is unrecognizable), such data is not protected as personal data. In such cases a notice is not obligatory however the Commissioner advises a notice to be published anyway, so as to avoid potential marginal situations where individuals may still be identified from the recorded material.

Question: What if I perform video surveillance at home and only monitor my private property. Do I still have to publish a notice?

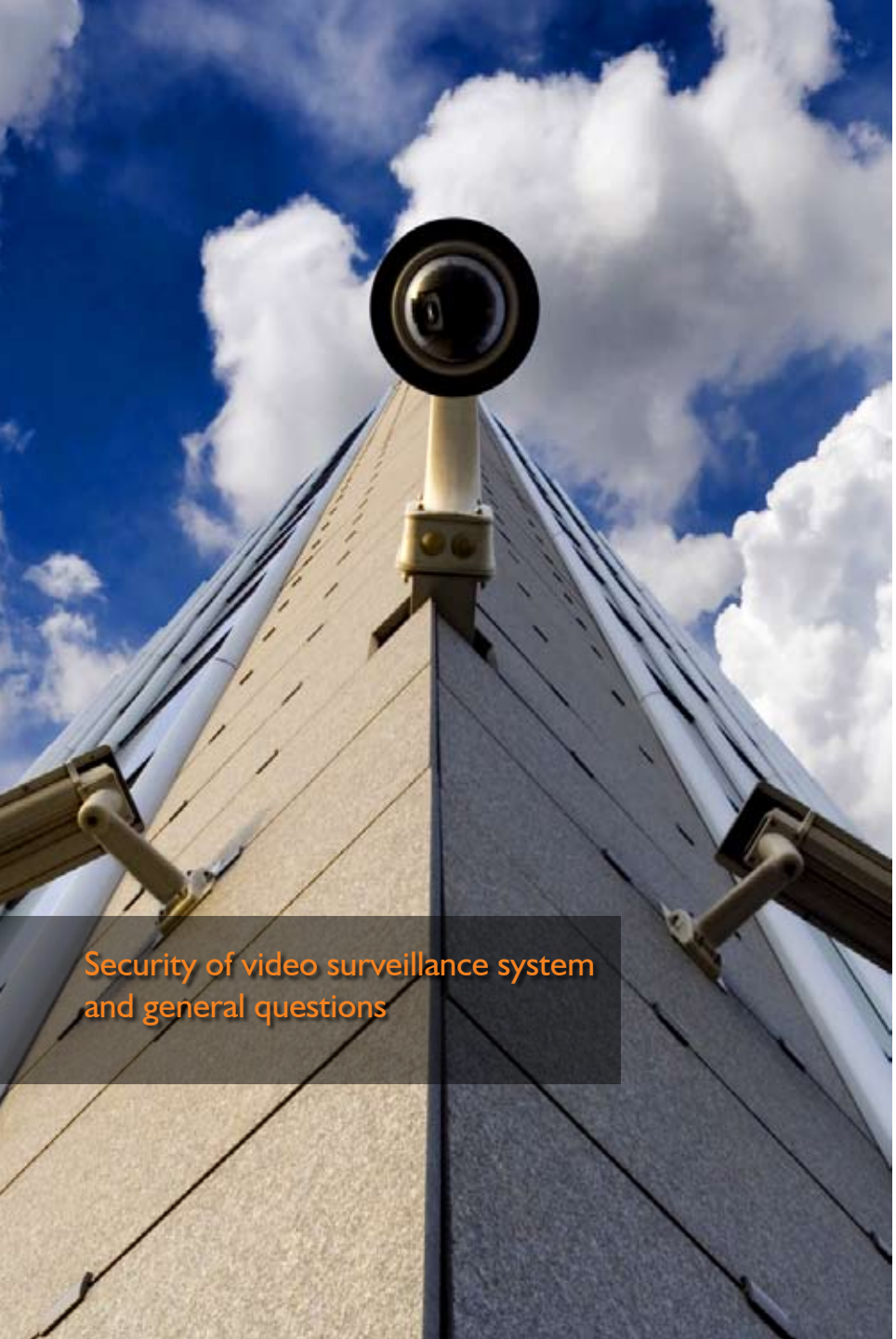
Answer: No, if you really are only monitoring your own private property.

Para 1 Article 7 of ZVOP-1 states that the act does not apply to the processing of personal data performed by individuals exclusively for personal use, family life or for other domestic needs.

In the case of monitoring of private property (may it be the house or other private premises) the Commissioner sees no reasons that would prevent or prohibit such use of video surveillance means. The cameras should however not target the areas where other people are moving or areas used by neighbours for utility purposes. If a person is monitoring other people in the area used for utility purposes, or outside of the private property, without their permission and without their knowledge, this might constitute a criminal act. According to Article 134 of the Obligations Code (Official Gazette RS, no.83/01) the injured individual may start legal action before the competent court which may then order the acts (e. g. video surveillance) that impinge on human rights to personality, personal and family life or other human rights, to terminate. Monetary penalties are also applicable. Similarly the Penal code (Official Gazette of RS, no. 95/04) in Article 149 provides that whoever unlawfully visually records or makes footage of another person or the persons' premises without the persons' consent and thereby significantly interferes with this persons privacy, is punished by a fine or imprisonment for up to one year.

Question: Can the notice on video surveillance of official office premises and business premises be published in the internal act on personal data security?

Answer: Yes, but this notice will be only considered as part of the internal act and not as a notice as defined by the Article 74 of ZVOP-1.



Security of video surveillance system and general questions

Question: How should video surveillance system be protected to fulfil the obligations defined in ZVOP-1?

Answer: The Commissioner emphasizes that the rules for the security of video surveillance system as well as for security of individual footages are the same as the rules for personal data security in general. Security of personal data is described in Articles 24 and 25 of ZVOP-1, for contractual data processors also in Para 2 Article 11 of ZVOP-1.

More information on data security is accessible in a manual on data security, published by the Commissioner on its website http://www.ip-rs.si/publikacije/prirocniki/, under the topic »Let's secure personal data, a manual for data controllers.

Question: Do we have to keep records of the use of material made by the video surveillance system, and are there any recommendations regarding this?

Answer: Yes. According to Article 25 of ZVOP-1 any legal or natural person performing video surveillance has to define in the internal acts the person responsible for establishing a record of video surveillance, and the persons who, due to the nature of their work, may process the data contained in the record of video surveillance.

It is recommended that the records of video surveillance contain the following information on each individual access (transmission of data, only access to data, etc.) to the content of video surveillance: serial number of the access or transfer, the name and surname of the person who accessed the footage, date of access, the purpose of access, data on the time period of acquired images (from-to) information about who, when and on what legal basis was provided with the footage, the medium on which the images were transmitted (CD, floppy disk, etc..), potential remarks, if any, and the signature of an authorized person.

A very useful template may be appendix 2 (click) to the Regulation on the measures of private security (Official Gazette of RS, no. 75/2004).

Video surveillance, generally

Question: What is the definition of video surveillance – is it necessary to record the images or is mere live video transmission also considered as video surveillance?

Answer: Para 1 Article 74 of ZVOP-1 provides that the chapter on video surveillance applies to implementation of video surveillance, if not stipulated otherwise by the law. In the context of video surveillance where the images are not recorded (not even for a very short period of time), the question is, whether this is a filing system. ZVOP-1 in the introduction provides that it only protects personal data that are part of a filing system. In video surveillance, conducted as a live video transmission (e. g. without recording images) no filing system is established and therefore such video surveillance does not fall under the definition of data processing as defined by ZVOP-1. The Commissioner however advises, that the operator of video surveillance even in this case publishes a notice for the individuals who enter the monitored area, so as to let them know they are being monitored in real time. This is important because the individuals that have been secretly video monitored have the right to judicial protection.

Question: Can high schools implement video surveillance with real time transmission in the corridors without pupils or their legal representatives consenting to this, and with every teacher having access to the live transmission? Can the high school in this case record the images?

Answer: Yes, but it is nevertheless necessary to notify all the employees on the implementation of video surveillance (Article 74 of ZVOP-1) and to define the person(s) responsible for the records of video surveillance. Not every teacher can have access to these images at any time.

To implement video surveillance in the corridors, the school does not need the pupils' or their representatives' consent. The conditions set by Article 75 of ZVOP-1 need to be respected even in the case of access to the recorded material. Bearing in mind the proportionality principle (Article 3 of ZVOP-1), it is only admissible to access the recorded material in the event of those conditions set for access to the footages of official business premises video surveillance. Only the authorised person (for example the director) may access the recorded material, only if 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 (Article 75 of ZVOP-1). Any access, copying or supply of the material to a third person has to be included in the video surveillance log.

Question: How long can we store the video surveillance footage for?

Answer: For as much time as defined in the Internal act on personal data security or other similar act, but for maximum of 1 year after the creation of the footage. Then the data has to be erased. This applies to the video surveillance of access to official office premises and business premises. To other video surveillance the general retention period applies. Article 21 of ZVOP-1 stipulates that personal data may only be stored for as long as necessary to achieve the purpose for which they were collected or further processed. The Commissioner advises that the retention period be as short as possible. Most of the data controllers store the data on video surveillance for between 7 days and 3 months.

Question: What about students who work for the employer? Do they count as employees in terms of video surveillance?

Answer: No, the students are not considered as employees, but all the provisions of Article 74 of ZVOP-1 have to be respected anyhow.

Question: I fulfilled the conditions for implementation of video surveillance, I published a notice to that effect, I notified the employees in writing. Have I done everything that's necessary?

Answer: No, the filing system that is created needs to be secured (more in the chapter on security of the video surveillance system) and in some cases (explained below) you need to establish a filing system catalogue (for every filing system) and supply this data to the Commissioner (http://www.ip-rs.si/varstvo-osebnih-podatkov/register-zbirk/). In some cases you also have to establish an Internal act on personal data security (a template is available here http://www.ip-rs.si/obrazci/varstvo-osebnih-podatkov/).

As provided by Para 4 Article 7 of ZVOP-1, data controllers with less than 50 employees are exempt from the obligation of establishing an Internal act on personal data security, establishing the filing system catalogue and reporting the data from the catalogue to the Commissioner. Para 5 Article 7 of ZVOP-1 defines the data controllers who are not exempt from these obligations:

- data controllers in the public sector,
- notaries public,
- attorneys,
- detectives,
- bailiffs,
- private security providers,
- private healthcare workers,
- healthcare providers,
- and data controllers that keep filings systems containing sensitive personal data and processing of sensitive personal data is a part of their registered activity.

Question: We implemented a video surveillance system but we do not record the material, the security guard is watching the footage in real time. It is basically just "remote eyes" surveillance. What are our obligations under ZVOP-1?

Answer: According to a ZVOP-1 you do not have any obligations; however we recommend you to publish a notice that the area is monitored.

As follows form the introductory provisions of ZVOP-1 (see points 3 and 5 of Article 6), this act only applies to personal data that are part of a filing system. In the »remote eyes« system the filing system does not exist, therefore it cannot be regarded as video surveillance in the sense of ZVOP-1.

Question: My neighbour is constantly monitoring my bedroom window with a security camera, and I don't have shutters on. Is he in breach of ZVOP-1?

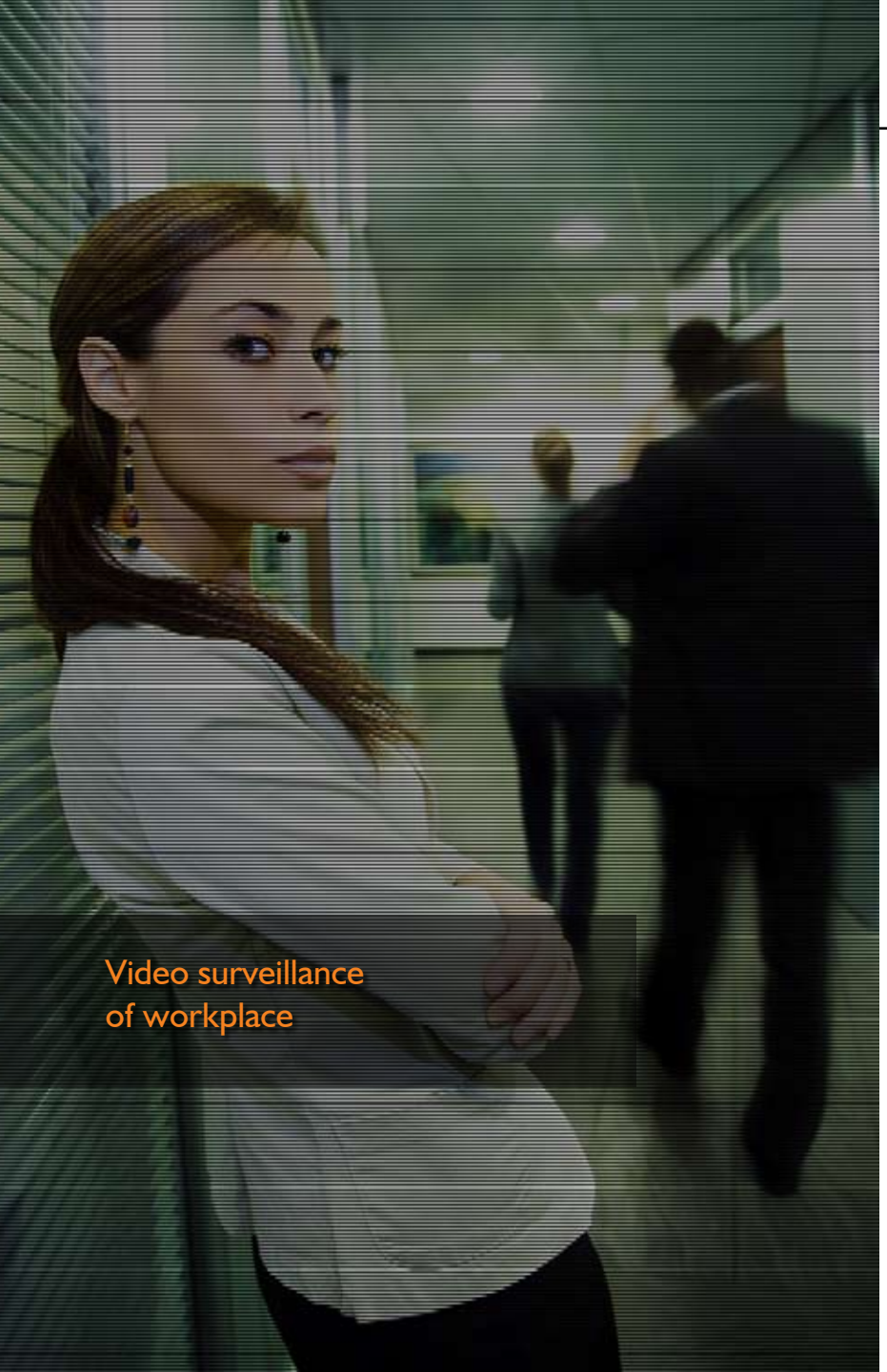
Answer: No, but with such activities the neighbour risks a criminal charge or a lawsuit.

ZVOP-1 is a sectoral law, governing video surveillance in Articles 74 to 77. However the general provisions of ZVOP-1 also stipulate when this act applies and when it does not. In Article 7, ZVOP-1 provides that it does not apply to the processing of personal data performed by individuals exclusively for personal use, family life or for other domestic needs. ZVOP-1 thus does not apply in cases when individuals perform video surveillance for their domestic need (see Para 1 Article 7).

However the fact that ZVOP-1 does not apply in this situation does not mean that individuals do not have access to legal remedy if they believe their right to privacy has been breached. If the operators of video surveillance record other people without their permission they are criminally liable. According to Article 134 of the Obligations Code (Official Gazette RS, no.83/01) the injured individual may start legal action before the competent court which may then order the acts (e. g. video surveillance) that impinge on human rights to personality, personal and family life or other human rights to terminate. Monetary penalties are also applicable. Similarly the Penal code (Official Gazette of RS, no. 95/04) in Article 149 provides that whoever unlawfully visually records or makes footage of another person or the persons' premises without the persons' consent and thereby significantly interferes with this persons privacy, is punished by a fine or imprisonment for up to one year.

Question: Does video surveillance, performed by contractual security companies, fall under contractual data processing?

Answer: Yes. When video surveillance is entrusted to an outsider (such as a security company) you should not overlook the provisions of Article 11 of ZVOP-1. The security company is in this case a contractual personal data (recorded images) processor, who processes data on behalf and in the name of the client. The client or data controller may by contract entrust individual tasks related to processing of personal data to a data processor that is registered to perform such activities and ensures the appropriate procedures and measures pursuant to Article 24 of ZVOP-1. The data processor may perform individual tasks associated with processing of personal data within the scope of the client's authorisations, and may not process personal data for any other purpose. Mutual rights and obligations must be arranged by a contract, which must be concluded in writing and must also contain an agreement on the procedures and measures pursuant to Article 24 of ZVOP-1. Data controller/client oversees the implementation of these procedures and measures. In this situation it is of vital importance that the contractual data processor performs individual tasks associated with processing of personal data only within the scope of the client's authorisations, which must be clearly defined by a contract. The data processor may not process personal data for any other purpose. Otherwise it could soon happen that the security company would start using the recorded material for purposes outside of the authorisation. In such case the data controller can be fined for a number of offences, regarding contractual data processing, video surveillance and data security. Article 11 of ZVOP-1 also stipulates that in the event of a dispute between the data controller and the data processor, the data processor is bound on the basis of a request from the data controller to return to the controller without delay the personal data processed under contract. In the event of cessation of a data processor (bankrupt, etc.), personal data shall be returned to the data controller without unnecessary delay.



General information about privacy and personal data protection in the workplace

Taking into account the principle of proportionality, it is necessary to establish in each individual case, whether there is a less intrusive tool available instead of video surveillance of the employees workplace. The European Court of Human Rights in the case of Halford v. United Kingdom (25/06/1997, Reports 1997-III) thus stated that a person can have a reasonable expectation of privacy even in the workplace.

The question of privacy protection in workplace always has to be considered on a case by case basis, because there are two legitimate interests involved. The right of the employer to oversee the use of his property collides with the right of the employee to privacy and data protection, who can reasonably expect a degree of privacy and independency even at workplace. The Constitutional court of the RS has used the proportionality principle and stated that when protected rights collide it is not a priori permissible to use any measures to protect one right when the other right deserves the same level of protection. In collision only proportional encroachments upon one right are permissible, such that do not protect the other right absolutely but only to such extent that both of the rights limit each other proportionally.

In protecting the right of the employer it is thus necessary to also consider the right of the employee to privacy. Therefore the protection of the employer's interests may not be implemented with measures that would completely deny the employee the right to privacy at workplace. And on the other hand the right of employee should also not prejudice the rights of the employer to monitor the use of his assets. After all there are two constitutional rights in question (Article 35 (and further) of the Constitution of RS – the right to privacy; Article 67 of the Constitution of RS – the right to property).

A decision of the Commissioner in one of the cases:
The Commissioner finds that the data controller has violated the individuals' privacy by installing the video cameras in such positions as to directly and continuously record them. The data controller has violated the principle of proportionality because he processed personal data (an image of an individual is by all means personal data) of individuals in the scope that exceeded the scope needed to fulfil the purpose of video surveillance, such as defined by the data controller. This purpose could have been achieved with less invasive means. Considering that less invasive means to achieve

the purpose of video surveillance exist, the data controller is in breach of the part of Para 1 Article 77, which stipulates that video surveillance may be implemented if the purposes cannot be achieved by milder means. The Data Protection Supervisor emphasizes that in this case a less intrusive measure, which would protect the integrity of the employees, would be for the surveillance system to stop recording during the working hours set by the employer. During this time a number of employees are present in the monitored area and the danger of assets being stolen is smaller than at hours when the employees are not present. This way employees working in the monitored areas would not feel such psychological pressure during work process, which is emphasised by the labour union. This solution would enable the employer to protect his property at times when danger of theft exists; at times when there is no work process going on at the premises.

Answers to specific questions

Question: Is it allowed to create a website that would transmit live happening from my own bar on the internet?

Answer: If you wish to implement surveillance cameras that would transmit real time happening from your bar to the internet you have to - depending on the installation of the cameras – respect the provisions of Articles 74, 75 and 77 of ZVOP-1. If you will not monitor the access to the premises or workplaces than it is enough to publish a notice with all the elements prescribed by Para 3 Article 74 of ZVOP-1.

In such cases it is necessary to understand the difference between video surveillance governed by ZVOP-1 and filming the happening in the bar for other purposes, such as television shows, where the rules of ZVOP-1 do not apply. However even in such cases it is obligatory to notify the visitors of the bar that video recording takes place. Otherwise you might be criminally liable or risk a lawsuit.

However, if you install the cameras in such a way that they record access to business premises (entrance of the club) and inside workspaces at premises (bar counter, tables ...), you need to meet all legal conditions set in Articles 75 and 77 of ZVOP-1. In the first case you need to inform all the employees about video surveillance taking place and publish a notice from Article 74 of ZVOP-1. Whereas in the second case, when the cameras are installed in a way to also record employees, it is vital firstly to establish whether there are reasons for such surveillance of workplace. It is urgent to emphasise that a bar is a specific place where the entire bar is the workplace of some employees. Article 77 of ZVOP-1 provides that you can only perform video surveillance within work areas 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 milder means. Additionally the employer has to seek advice of the representative labour union if such exists at the employer. The Commissioner emphasises that in such cases it will be difficult for the employer to pass the inspections test on the reasons for implementation of video surveillance as defined by Article 77 of ZVOP-1.

Question: Is it allowed to video monitor employees for the purpose of research without their knowledge?

Answer: No.

Considering the conditions for lawful video surveillance the employer may only monitor the employees for the purposes and under conditions set in ZVOP-1. The purpose of »research« is too vague and not specified by the law, therefore the Commissioner believes that such video surveillance, if the material is stored and if the individuals may be identified from the footage, is not permissible.

If you record other people without their permission you may be criminally liable. According to Article 134 of the Obligations Code (Official Gazette RS, no.83/01) the injured individual may start legal action before the competent court which may then order the acts (e. g. video surveillance) that impinge on human rights to personality, personal and family life or other human rights to terminate. Monetary penalties are also applicable. Similarly the Penal code (Official Gazette of RS, no. 95/04) in Article 149 provides that whoever unlawfully visually records or makes footage of another person or the persons' premises without the persons' consent and thereby significantly interferes with this persons privacy, is punished by a fine or imprisonment for up to one year.

Question: Is it allowed for the employer to perform video surveillance in a way that the employees do not know where the cameras are installed, under the condition that they have been notified on video surveillance?

Answer: In principle, yes.

The purpose of the notification from Article 74 of ZVOP-1 is primarily in the fact that the individual is aware of video surveillance, but not necessarily about exactly where the cameras are physically located. Therefore, a "secret" video camera would not be controversial if installed in such a way that would not in any way interfere with privacy of individuals, for example at the entrance to a building. However, even in this case – of entrance to business premises- the employer should inform the employees on the installation. If the employer does not do that and installs the cameras in a way that they record access to the official business or commercial premises, the employer violates the above mentioned Article 75 of ZVOP-1, in the part where he is obliged to notify the employees on the implementation of video surveillance. The employer would have violated ZVOP-1 also if he installed the cameras in a way that they record workspace, and he didn't firstly consult with the representative labour union, besides notifying the employees in writing.

If the employer does not violate any of the above, he can then set the cameras in a way that is invisible, but only on condition that he firstly pre-determined the area that is being monitored and notified the employees, and consulted with the representative labour union. The Commissioner especially stresses that the employer must not install video cameras in places where that would violate the privacy of the individuals, such as in the changing rooms, elevators or sanitary facilities.

Question: Is the employer allowed to hire a company conducting »mystery shopping« to video record the work of employees?

Answer: No.

The employer is often (if not always) the stronger party in the relationship to the employee. That is why it is strictly necessary to abide by the rules set by the Labour Relations Act (Official Gazette of RS, no. 42/2002; ZDR) even in the part, when it limits employees' personal data processing. Para 1 Article 46 provides that employees' data can be gathered, processed, used and provided to third persons only if this Act or other laws stipulate so, and if it is necessary in order to exercise the rights and obligations arising from employment relationship or related to employment relationship. This provision must be read together with the principle of proportionality from Article 3 of ZVOP-1, which provides 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.

In the specific case the purpose is clear – checking on employees, their work and attitudes to the customers. However it is vital to respect the rules for secret video surveillance.
Firstly it needs to be established that in this case this is video surveillance of persons and not work places as defined in Article 77 of ZVOP-1, where it is provided when and under which conditions it is permissible to implement video surveillance of workplaces: only when necessarily required for

- the safety of people or property or
- to protect secret data and
- business secrets.

We can easily conclude that control over the employees work with »mystery shopping« means, is not one of the above purposes. That is why the Commissioner emphasises that any secret video recording as described would constitute a breach of ZVOP-1 and possibly a breach of Article 149 of the Penal Code, which defines the criminal act of unlawful video recording.

The Commissioner also calls attention to the situation where such video surveillance would be performed by a contracted third person in a form of contractual data processing. As was established above the employer does not have the right to perform mystery shopping with secret video surveillance. No one can transfer to another person more rights than he possesses, and therefore the employer also cannot authorise a third party to perform secret video surveillance on his behalf. This way the employer would exceed the rights he has and thus risked to commit an offence or be criminally liable.

Question: Is it allowed to perform video surveillance in classrooms in the course of exams and study?

Answer: Yes, but only if all the obligations and conditions from articles 74, 75 and / or 77 are fulfilled.

Given the above conditions that have to be met for lawful video surveillance, the Commissioner concludes that you may implement video surveillance of employees (in this case teachers or professors) and of the "business" premises (if we consider the classroom as a business premise where the equipment needs to be protected) in

accordance with ZVOP-1. In this case you would also be monitoring the students, which would have to be notified (by a notice from Article 74 of ZVOP-1), that they are entering an area that is monitored by video surveillance. The mere reason for video surveillance you mention (to simply monitor the students during exams and study) is however not sufficient for lawful video surveillance.

Question: ZVOP-1 requires that the employer consults with a representative labour union prior to the introduction of video surveillance. As an employer I did so, and received a negative opinion from the labour union. Can I still implement video surveillance?

Answer: Yes, if the requirements set in Para 1 Article 77 of ZVOP-1, on conditions for video surveillance of workplaces are met.

Para 5 Article 77 of ZVOP-1 provides that the employer has to consult with the representative union, but it does not require its consent. The Commissioner recommends, however, that the employers take account of views and the reasons of the labour union, and try to find a common position on the planned introduction of video surveillance.

Question: I want to introduce video surveillance of our work premises, but there is no representative labour union in our company. What happens to this requirement?

Answer: If there is no representative labour union, of course you don't need to consult. Although we suggest you fully harmonize video surveillance with the conditions for its lawful implementation.

Question: In the school corridor, above the students' lockers, we wish to introduce video surveillance. Considering that video surveillance of locker rooms is not permitted, we would like to know if it is permitted to perform video surveillance the way we described. The hall is not a typical locker room because the students only put their coats and shoes off there.

Answer: Yes.

According to Para 3 Article 77 of ZVOP-1 it is prohibited to conduct video surveillance in workplaces outside of the working area, especially in the changing rooms, lifts and sanitary facilities.

In your case the lockers are located in the school corridor and the students only put off the coats and shoes there. That is why this area cannot be regarded as a changing room, separated from other spaces, in the sense of Article 77 of ZVOP-1 and thus video surveillance is not prohibited. You may perform video surveillance in the way described above, however the Commissioner advises you to pay attention to all the provisions for lawful implementation.

Question: Is it allowed for the security cameras at the cashier's desk to record the PIN codes?

Answer: No.

Retailers do not have the right to process the data on PIN numbers and therefore no PIN numbers should be in their filing systems (specifically in their video surveillance filing system), as the risk of abuse is too big. The purpose of security cameras is to protect the property and to monitor the cashiers and how they handle the money. That is why the cameras should be, following the principle of proportionality, installed in such a way that they do not monitor the narrow area of the keyboard, where customers type in their PIN numbers. If this is not possible, a barrier should be installed on the terminals that would prevent the cameras from recording the PIN.

When monitoring the cashier's desk the terminal for PIN codes has to be protected with a barrier.

Video surveillance and apartment buildings

Question: Can we monitor the entrance to an apartment building with a security camera?

Answer: Yes, if you fulfil the conditions from Articles 74 and 76 of ZVOP-1. Under these conditions you can perform video surveillance by yourself, however most commonly this is done by professional and registered security companies. These companies install and manage the security cameras in the name and on behalf of their clients – the data controllers. The data controllers may by contract entrust individual tasks related to processing of personal data to a data processor that is registered to perform such activities and ensures the appropriate procedures and measures pursuant to Article 24 of ZVOP-1. Those are organisational, technical and logical-technical procedures and measures to protect personal data, and to prevent accidental or deliberate unauthorised destruction, modification or loss of data, and unauthorised processing of such data.

Under the above conditions from ZVOP-1 the residents of apartment buildings may perform video surveillance of the entrance. They can monitor by themselves or hire a registered company to monitor on their behalf, on a basis of a contract.

ZVOP-1 allows video surveillance footages to be transmitted to a remote computer, however only authorised persons should have access to this data (for example one or more authorised residents, or an authorised employee of the contracted company). This way the residents will achieve protection of people and property compliant with ZVOP-1.

Question: How should we understand Para 4 Article 76 of ZVOP-1, if applied to the use of video intercom? Is it prohibited?

Answer: Para 4 Article 76 of ZVOP-1 states that it is prohibited to enable or implement current or subsequent examination of recordings of video surveillance systems through internal cable television, public cable television, the Internet or the use of other telecommunications means able to transmit such recordings.

The Commissioner at this point firstly notes that it is important to define the term telecommunications means. The Electronic Communications Act (Official Gazette of the RS, no 43/04, with amendments, hereinafter ZEKom) is the sectoral law in this field, however, it does not define the term telecommunications means. Its predecessor, the Act on Telecommunications (Official Gazette of the RS, no. 30/01; expired

on 1. 2. 2004; hereinafter ZTel-1), defined the term in point 24 Para 1 Article 3, as broadcasting, transmission, transfer, reception and direction of all kinds of messages in the form of signals, voice, image or sound with appropriate technical means.

Even the Dictionary of Slovenian language provides a similar definition:

Telecommunications – 1. Distant exchange, supply of information with the use of electromagnetic systems: enabling telecommunications, international association for the telecommunications, radio, and telephone telecommunications 2. An asset that allows the exchange, dissemination of information: the transfer of information via telecommunications.

Given these two definitions, "the telecommunications" involve the following conditions:

- there must be an exchange of information, an exchange is also broadcasting, transmission, reception, direction;
- the exchange must involve an electromagnetic system, or technical means;
- an information includes all forms of communications in the form of signals, voice, images or sounds.

All of the above conditions certainly apply to the video intercom:

- a camera that is installed at the entrance of a building, and it transmits a signal
- to the screen in an individual's flat;
- an exchange takes place between the camera and the device in the house, both are based
- on electromagnetic system and are technical means;
- information that is transmitted, is in the form of a signal, image, voice and sound.

Therefore it is indisputable that a video intercom is a telecommunications means used to transmit images. However, taking into account the Para 4 Article 76 of ZVOP-1 we can conclude, with the use of the so called logical explanation, that ZVOP-1 makes a difference between two systems:
- video surveillance system without the transfer of data (images);
- video surveillance system, that uses internal cable television, public cable television, the Internet or the use of other telecommunications means able to transmit such recordings.

The Act therefore distinguishes between 2 systems. In the first system all legal conditions governing the introduction of video surveillance need to be respected: ZVOP-1 here defines video surveillance that may be implemented only (the Commissioner's comment) when necessary for protection of people and property.

The second system, different from the closed system above, refers to the cable television and the Internet, brought to individuals on other legal bases (such as a contract). Because these two platforms are widely accessible and because it is impossible to control the access to the materials, the legislator prohibited transmission of video surveillance footage via these means.

Considering all the above the video intercom belongs to the second system, which do not fall under video surveillance as governed by ZVOP-1. The intercom's purpose is entirely different (it allows for the recognition of visitors), from the task of maintaining the video surveillance footage for the purposes of protecting people and property, which can be examined by authorised persons in an event of damage, and used as evidence.

Question: How should we understand Para 1 Article 76 of ZVOP-1, in particular, what to do when we collected 50% of approvals under the old legislation when this was enough – do we have to collect the remaining 20%?

Answer: You must obtain the consent of the remaining 20% co-owners.

The law is very clear in this part – you need consent from 70% of co-owners. If you have not obtained consent, the introduction of video surveillance is unlawful, regardless of whether the previous act stated otherwise. The legislator has obviously wanted to protect the rights of individuals, with regard to video surveillance in apartment houses being a relatively strong interference with the privacy of an individual. It is therefore necessary to achieve the broadest possible consensus. Therefore to avoid potential complaints you are advised to obtain the missing consents or terminate the surveillance.