Project implemented by Human Dynamics in association with:
IPS Institute
AlmavivA S.p.A.
Czech Office for Personal Data Protection
Privacy International

Project office:
Directorate for Personal Data Protection
10, Samuilova, room nr. 7 ,1000 Skopje
Tel: (+389) 2 3244 761
Email: ipa_dzlp@dzlp.mk

Document 2.1.4 - 4

GUIDELINES REGARDING THE PROCESSING OF PERSONAL DATA BY MEANS OF VIDEO SURVEILLANCE

Component 2

Activity 2.1.4 - 4

Table of Contents

I. INTRODUCTION

This code/guideline set the basic principles and guidelines for the effective protection of privacy with regard to the processing of personal data by means of video surveillance systems in accordance with the Law on personal data protection (hereinafter "LPDP"). Video surveillance is a part of various systems which monitor several areas of human activities – from road traffic, shopping, street movement banks, hospitals, control eployees to control security up to prevention of thefts and robberies, and many others. During this monitoring personal data are mostly to be processed.

What is the purpose/aim of this document?

This document aim is to demonstrate that video surveillance is only one part of the surveillance of society. There are several other techniques for monitoring and profiling of individuals. The main interest of data protection supervisory bodies is to focus on surveillance of individuals on the basis of camera system. In modern society the use of computer-based system and communication technologies allow the access to private and restricted areas.

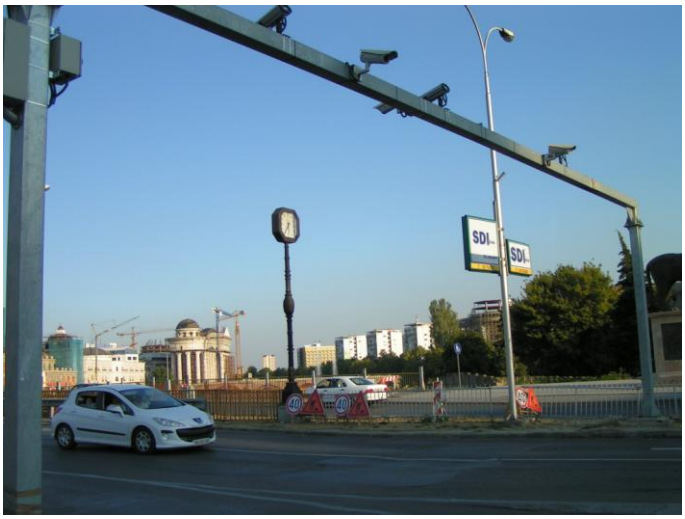
The level of surveillance of public areas has increased rapidly over recent 20 years, and continues further. The development of digital surveillance technology means that the nature of surveillance has changes dramatically during last decade. Digital surveillance means that the system is capable to capture the data about individual and transfer them everywhere for further processing. Modern surveillance systems use networked and digital cameras - camera is connected to internet, computer, telecommunication equipment, RFID, facial recognising system, an so like. Also this example shows that it is necessary inform broad public about new possibilities of modern surveillance systems and they risks to privacy of citizens.

Camera system installed on building

Protecting privacy and personal information means protecting individuals' rights to control how personal information is collected, used, stored and passed on. Protecting privacy also includes information security– protecting the confidentiality, integrity and availability of personal information. To be considered privacy-secure, an identification system must be designed to satisfy both of these parameters.

Video-surveillance is frequently used for various applications in current society. Many times the purpose of video-surveillance system is declared for public and individual security, fighting against crimes, prevention of thefts. Several times this purpose is only declared but the real use is different, the system is used for monitoring of individuals, surveillance of private activity of individual, monitoring effectiveness of work of employees, etc. Very often declared purpose is not fulfilled and the system purpose is far different from this which is notified to supervisory authority.

One of the major problems of the installation of video surveillance system is that individuals are not informed on such system installation and its purpose(s). The system is hidden and no information is provided. However, all advantages entail new problems that need to be addressed – e.g., who is owner of personal data used in the system; who is responsible for the accuracy and security of the data when the system is accessible to a number of other entities; where is the limit for sharing different applications into one storage memory, where are risks to private life of individuals, and so on.



Camera system monitors a public traffic

Videosurveillance monitors the movement aroud houses

Legal background

Everybody who has intention to install video surveillance system must be aware that such system falls under relevant provisions of the Law for Personal Data Protection (the LPDP contents some provisions related to protection of personal data by video-camera surveillance systems).

The controller who performs the video surveillance shall be obliged to display a notification. The notification has to be comprehensive, visible and displayed in such a manner to enable the personal data subjects to acquaint the performance of video surveillance.

The controller may solely perform video surveillance in an area necessary for fulfilling the aims of its setting.

The videos made while performing video surveillance shall be preserved until fulfilling the purposes of its performance, yet not exceeding 30 days, unless longer period is envisaged by another law.

The controller may perform video surveillance in official or business premises if it is necessary for:
- protection of the human life and health;
- property protection;
- protection of the life and health of the employees due to the job nature or
- provision of control over the entry and exit from the official or business premises.

The controller shall obligatory notify the employees for the performance of video surveillance in the official or business premises.

It is prohibited to perform video surveillance in dressing rooms, fitting rooms, toilets and bathrooms, elevators and other similar areas.

For the purpose of performing video surveillance in single and multiple quarter buildings, it shall be necessary to obtain a written consent of all owners, or lessees of the quarters.

It is prohibited to record the video entrances in personal apartments of other owners, that is lessees.

Information about monitoring a space

To whom these guidelines are addressed?

These Guidelines are addressed to data controllers, data processors and whatever companies who installed and operate camera system and thus process personal data by the means of video cameras. However, also data subjects and broad public who are subjects of video surveillance systems have right to be informed about technical and legal conditions of such systems and find a number of information regarding the fulfilment their rights given to them by the Law on Personal Data Protection. We hope that this document is useful also for Data Protection Officers and other data protection experts.

Application of these Guidelines

This Guidelines shall apply to any video-camera systems operate by public and private bodies when the images relate to living individuals (data subjects) and are captured and stored in recording technology. These Guidelines are not apply to:

- video-phone calls and video-conferencing;

- simple video-entry systems without recording; *)

- camera use for artistic or journalistic purposes (e.g. film making, broadcasting newsworthy events, etc.);

- recording or broadcasting events such as conferences, seminars, meetings, and training activities for documentary, education and similar purposes of such activities;

- recording of internal meetings (as example the management) of public and private bodies;

- surveillance by mobile phone, telecommunication equipments, smart cards and RFID tags, loyalty cards, banking transaction, passengers identification (in public transport, air passengers, etc.) and any other forms.

Under the scope of this Guidelines comes also using any other electronic device or system, fixed or mobile, if it is capable of capturing image data (as example portable video-cameras, cameras taking still images, webcams, infra-red cameras, or heat recognition devices).

How video surveillance is defined?

The video surveillance is defined as the monitoring of a specific area, event, activity, or person by means of an electronic device or system for visual monitoring. Video-surveillance technology system refers to cameras that monitor or record the activities of individuals, including but not limited video cameras; closed circuit television cameras (CCTV); digital cameras; and time-lapse cameras. These devices may be used to create records, incl. videotapes, photographic or digital images. The video surveillance systems may be used by public authorities on public spaces for crime prevention or even crime prosecution as well as private bodies for various purposes.

III. GENERAL PRINCIPLES FOR PROCESSING

What are basic rights of citizens?

It must be reminded that video surveillance systems deal with personal data about individuals, thus some human rights, including the right to privacy, shall be taken into account. Than, all data protection legal principles shall be apply to these systems. Video surveillance in public spaces concerns also to free movement of individuals. This right is provided for of Additional Protocol to Additional Protocol to ECHR. This freedom not only concerns the right to move freely in physical space but also the right to move constantly being traced.

Protecting privacy also includes information security–protecting the confidentiality, integrity and availability of personal information.

Data controllers and/or operators following issues must determine in advance of installing video surveillance technology:

- is the camera demonstrably necessary to fulfil a specific aim or purpose?
- it is likely to be effective that meeting that need or purpose?
- it is an alternate method to achieve that aim? (less privacy intrusive in particular)
- it is degradation of privacy in balance to the benefit gained?

In using video surveillance systems as a technology used for personal data processing, it is necessary to stipulate legislative, ethical and other rules for the protection of such data from unauthorised access, modification, publication or any other unauthorised processing.

Center of street surveillance system

Principle of fair processing – what it is about?

The collection and processing of personal data by means of video surveillance should be fair and lawful. Only the personal data necessary for the fulfilment of the purpose(s) for which the systems is created should be collected and stored on the system storage media. Systems using video surveillance should be transparent to the data subjects whose personal data are stored and processed. Fair and lawful principle requires:

1. Video surveillance should only be deployed to address a real, pressing, and substantial problem.

2. Video surveillance should be viewed as an exceptional step, only to be taken in the absence of a less-privacy invasive alternative.

3. The impact of the proposed video surveillance on privacy should be assessed before it is undertaken.

4. The camera location should be chosen to minimise viewing areas that are not relevant for the intended purpose(s).

5. Public consultation should precede any decision to introduce video-surveillance.

6. The video surveillance must be consistent with applicable laws.

7. The video surveillance system should be tailored to minimize the impact on privacy.

8. Fair information practices should be respected in collection, use, disclosure, retention and destruction of personal information.

9. Excessive or unnecessary intrusions on privacy should be discourages.

10. The right of individuals to have access to their personal information should be respected.

11. The video surveillance system should be subject to independent audit and evaluation.

12. The public should have a right to know about the video surveillance system that has been adopted.

Data subject has the right to be informed

Where personal data are collected and stored by video surveillance system, the data subject should be informed of the purposes of processing, the identity of the controller, the categories of data concerned and the recipients or categories of recipients of the data that are stored. Other information should be provided to the data subject, where this is necessary to guarantee fair processing of personal data.

The personal data subject may anytime request from the controller to inform him/her on the scope of personal data or categories of processed personal data related to him/her, on the purpose(s) of processing personal data, means of processing (see articles 10, 11, 12 of LPDP).

Information to data subject must be provided in an intelligible form, using a clear and plain language, in particular for any processing addressed specifically to minors.

The controller shall respond to the abovementioned request in accordance with the LPDP within 15 days.

Data subjects should always be informed that they are about to enter an area under video surveillance; this also applies to events and/or public shows (e.g. concerts, sports events, etc.).

To that end, the DPA considers that the same simplified model of "minimal" information notice – where the data controller and the purpose of the processing are specified – can be used as described in the LPDP (article 9-a); a facsimile model notice is shown in Annex 1 to this Law. The above model notice can obviously be adjusted to the specific requirements. If several cameras are deployed and the area under surveillance is especially large, and by having regard to the filming arrangements, several notices may have to be posted.

Data must be complete, correct and update

The principle of accuracy means that personal data collected and process by video surveillance technology shall be accurate and, where necessary, kept up to date. Personal data captured in video surveillance system is not allowed to modify or change befor further processing. Personal data, which is inaccurate, incomplete, or not up to date having regard for the purpose for which it was collected or for which it is processed , is erased or rectified. In video surveillance system the data already recorded and stored in the storage memory shall be regarded "up to date" even they were collected in some past time. It is not allowed any manipulation followed to modification of data.

Upon the request of the personal data subject, the controller is obliged to supplement, amend, delete or prevent the use of the personal data, if they are incomplete, incorrect or not updated and if their processing is not in conformity with the provisions of the Law (article 14 of LPDP). However, in case of video surveillance, the application of this principle in practice is difficult to be realised.

Information in the case of disclosure

In addition to the essential information, when data are intended to be communicated to third parties, data controllers must ensure that data subjects are informed of:

- any recipients or types of recipients of the data and the purpose for which the data will be disclosed;
- their right to object to from disclosing for specific purposes (for instance for direct marketing).

This information should be given at the time of collection, and every effort should be made to do so, but where this might be difficult or impossible this information should be given before any such communication to third parties takes place.

When a video surveillance is created, the data subject should be properly informed about how the system works and what are they rights and duties.

The purpose of video surveillance must be specified

Before deciding to install new video-surveillance system the institution/company must first establish the purpose of the video-surveillance system and must make sure that this purpose is legitimate. The purpose which vague, ambiguous, simply to general description is not sufficient. Being specific about the purpose of the video-surveillance can help the institution/company to comply with the Law (LPDP) assess the success of the system and explain to its workers and the public why the system is needed. The institution/company must ensure that captured data will not be subsequently used for unforeseen purposes or disclosed to unforeseen recipients. It must be reminded that incompatible purpose do not only include new purposes altogether unrelated to the initial purpose, but also all such purposes which would not have been reasonably expected by individuals (data subjects) under the video-surveillance system (as example – when the camera-surveillance system purpose is the security, and as such was announced to employees, the recorded data should not be used to assess how well employees perform their job or whether they come to workplace on time).

Very often the video-surveillance system is deployed for "security purpose". In such a case the institution/company should carefully evaluate risks, and not merely state that the purpose is to "observe any anomalies inside the security area (e.g. building) or "to deal with security incidents". The data controller (system operator) should not only have a general idea of what it wishes to use the system for, but must have detailed conception of what they wish to use their system for. They must also have detailed ideas on security incidents that are expected to occur in the area (space) under surveillance.

Only authorised persons have the right to access

Only the person with authorization from the controller or processor, including the processor himself, may have the right to access to storage memory where data from cameras are recorded. Those persons:

- have to be introduced with the principles for personal data protection prior to accessing the personal data;

- perform the right to access in accordance with the directions received from the controller, unless otherwise regulated and
- shall preserve the personal data as confidential, as well as the measures for their protection.

The controller and processor shall be obliged to keep records for persons authorized for access to storage memory, containing: name and surname of the authorized person, date of issuance, expiry date, as well as scope of authorizations for approach to the personal data and access manner.

The authorised parson also contributes to fulfilment of all data protection principles pursuant to the LPDP.

The right of access to the storage memory and further use of recorded personal data is very sensitive issue. It is recommended that the access to the storage device is always realised by two authorised persons in coincident. The access made by single person shall not be allowed.

IV. MONITORING AT WORKPLACE

Some specific issues arise from monitoring of workers. It must be taken into account that employees have legitimate expectations that they can keep their personal lives private and that they are also entitled to a degree of privacy at the workplace.

In the context of a number of European Human Rights Court, we can say that the individual does not abandon his/her privacy and data protection every morning at the home doors when going to workplace. The individuals have a legitimate expectation of a certain degree of privacy also in the workplace. The work's relationships are a significant part of their relationship with other human beings within the workplace. However, this right must be balanced with other legitimate rights and interests of he worker, in particular its right to run his business efficiently to a certain extend, and above all, the right to protect himself from the liability or the harm that workers' actions may create. These rights and interests constitute legitimate grounds that may justify appropriate measures to limit employee's right to privacy. We can say generally that the surveillance rights of employer end where the constitutional (fundamental) rights of employee begin.

If the employer has intention to monitor its workers, it must be clear about the purposes and satisfied that the particular monitoring system is justified by real benefits that will be delivered. Employees should be always aware of the purposes of monitoring, about placing of cameras, about access to the recorded images. The reason of monitoring by camera system must be defined clearly and the benefit must be demonstrated. If there are others measures that constitute a lesser invasion of the data subject's (employee) privacy, such measures must be taken instead.

The employer shall be aware about Basic data protection principles which shall be met when video surveillance system is developed.

V. EXERCISING DATA SUBJECTS' RIGHTS

In democratic society, data subjects have the right to exercise their freedom of movement without undergoing excessive psychological conditioning as regards their movement and conduct as well as without being the subject of detailed monitoring such as to allow tracking their movement and/or triggering "alarms" based on software that automatically "interprets" an individual's supposedly suspicious conduct without any human intervention – an account of the disproportionate application of video surveillance by several entities in a number of public and/or publicly accessible premises.
The data subjects' rights as defined in the Law (LPDP) other regulation and this code/guidelines, including the right to object to the processing of his data for specific purposes including the possibility of not being contacted on behalf of someone else, object to the disclosure of data to a third party, access and to rectify data which are inaccurate, to claim the deletion or blocking of data when its processing does not comply with the provisions of the applicable legislation, to object the processing of data for different purposes, shall be exercised in the first instance before responsible person/officer of the data controller or processor, directly or through a representative.

The responsible person/officer must implement procedures to enable data subjects to exercise the rights provided in the law and/or this code/guidelines in a simple, fast and efficient way, which do not entail undue delay or cost nor any gain whatsoever for the responsible person.

When a responsible person concludes that pursuant to the law the exercise of rights under this code/guideline is not justified, the data subject should be informed of the reasons that led to this conclusion.

VI. SOME PRACTICAL ISSUES

In accordance wit common practice ion the EU as well as recommendation of European Data Protection Supervisor, also the DPDP advices some practical issues when the video-surveillance system is deployed. As the basic principle addressed to the system operator is that should be minimised any negative impact on the privacy and other fundamental rights and legitimate interests of those under video-surveillance system. The adequacy of each choice made should be verified and assessed with this view point.

Placing the cameras

One of key aspect is the placing the camera and its technical parameters. The camera shall be located to minimise viewing areas that are not relevant for the intended purpose(s). As example, when a camera is installed as to monitor the entrance of the controller's building it must be ensure that camera is nor able to record area of surrounding privacy areas of neighbouring. Another example – when a camera in installed inside the operator, controller's building than should be taken to ensure that the camera only relevant area of protection and not neighbouring private offices (like lavatory, kitchen, rest-room, cloak room, etc.).

Number of cameras

The number of cameras to be installed in the system will depend on the size of monitored area, the size of monitored buildings, on the level of security purpose and several variety factors. It is recommended to install the same types of camera as is appropriate of functioning system. When the number of installed cameras is disproportioned then the risk of likelihood of affect to privacy and other fundamental rights increases. It is recommended to limit a number of cameras to what is strictly necessary to achieve the purpose(s) of the system. The number of installed cameras shall be included in the document on the video-surveillance company policy.

Time of monitoring

The time when cameras of the system are set to record the images should be chosen to minimise monitoring at times that are not relevant for the intended purpose(s). As example, if the purpose of the video-surveillance system is security, whenever possible, the system should be set to record only during times when there is a higher likelihood that the purported security problem occurs. Take into consideration if the camera set to function only in now-working hours or during week-ends is sufficient to fulfil the purpose.

Resolution and image quality

The resolution and image quality of recorded data must be adequate to the purpose of the system. Different purposes require different quality of images. As example, when identification of the individuals is a crucial expected result of the system then the resolution parameter of the cameras, compression settings in a digital system, the location, the distance, the lighting and some other factors should be taken into account so that the result of quality of images is sufficient. On the other hand, if the identification of individuals is not prime effect of the system, the camera resolution parameters should be chosen so that no recognisable facial images are not necessary.

VII. The Directorate for Personal Data Protection

In the broadest sense, the Directorate for Personal Data Protection is responsible for proper implementation of the Law on Personal Data Protection. This means that the Directorate cares for personal data protection of the citizens and protects their rights.

This role is carried out by the Directorate through:

- resolving citizen's complaints for violation of their data protection rights throughout inspection;
- conducting inspection ex officio to check whether the data protection principles are implemented properly.

However, it should be noted that Directorate has not only repressive role – does not solely solve problems when they occur. Rather, the role of the Directorate is to acquaint citizens closer to their rights.

How to exercise the right to complain?

If data subject (natural person or citizen's association where the natural person is a member) is not satisfied with the responses and information given by responsible person/officer of the data controller, and considers that his/her rights provided in the Law and/or this code/guidelines are violated, or information provided insufficient s/he can submit a request to the Directorate for personal data protection (DZLP) for confirming violation.

The Directorate during the procedure shall decide whether to disclose personal data of the submitter of the request or personal or data of the witness, to the opposing side in the procedure.

Appendix

FAQs - Frequently Asked Questions

1. Why video-surveillance data fall under data protection legal regime?

We must take into consideration the definition of personal by provided by European Directive (95/46/EC) and the Law on Protection of personal data. These documents stipulate: “Personal data are defined as any information relation to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity”;

It means in practice, the data (images) collected from the camera surveillance system are in the same substance – they may identify individuals (directly or indirectly). The logical consequence is, such data must be adequately protected in compliance with data protection legal regime.

2. Do only permanent video surveillance systems come under the scope of legal duties and a Code of conducts?

No, the legal duties as well as this Guidelines apply even if the cameras are only used an ad hoc basis.

4. How select a proper camera lens?

The lens of cameras use in video surveillance system must be adequate to declared purpose(s). If you need security camera in the office or warehouse and you need to see as much as possible, you should go for 2.8 – 4 mm lens (wide angle). However, if you need to observe a limited area (like entrance doors, narrow view, view close to the object, etc.) you should go for 8 mm lens. The suitable cameras for your system depend on several parameters, the camera lens to be adjusted in accordance the purpose for which it is used.

5. What is Closed Circuit Television (CCTV)?

A CCTV or Closed Circuit Television refers to a visible or covert video system intended for only a limited number of viewers. In Closed Circuit TV (CCTV), the picture is viewed or recorded, but not broadcast. It was initially developed as a means of security for banks and casinos; however, today it has been developed to the point where it is simple and inexpensive enough to be used with Home Security Systems, and for everyday surveillance. More specifically, CCTV is a television transmission system in which live or prerecorded signals are sent over a closed loop to a finite and predetermined group of receivers, usually as scrambled radio waves that are unscrambled at the point of reception. CCTV takes numerous forms and performs a wide range of functions ranging from image enhancement for the partially sighted to the transmission of pay-per-view broadcasts. Although cable television is technically a form of Closed Circuit TV, the term is generally used to describe systems with more specialized applications than a standard broadcast or cable television. Such specialized systems are not subject to regulation by the Federal Communications Commission (FCC); however, Security Cameras using scrambled radio waves are in fact subject to common carrier tariffs and FCC conditions of service.

6. What is Remote Surveillance?

The ability to monitor your home or business from different location is called Remote Surveillance Capability. With our system you can monitor your location from a remote location through Internet.

7. What does a basic video surveillance system consist of?

A basic system usually has about 4 outdoor and/or indoor color cameras that are connected to a central digital video recorder (DVR) located on-site. The recorder can store information from days to weeks to months depending on options. The cameras themselves can have daytime only capabilities or daytime and night-time capabilities. The cameras can be “fixed” looking at a pre-defined area or “movable” - automatically patrolling a large, variable region through pan-tilt-zoom features that are user defined. The system can be viewed internally through a standalone monitor, computer, and/or most cable TV/satellite systems. Externally, the system can be accessed from anywhere in the world over the internet. Some systems have the capability to be viewed through a users Smartphone (iPhone, Blackberry, etc.).