Twinning project "Implementation of the best European practices with the aim of strengthening the institutional capacity of the apparatus of the Ukrainian Parliament Commissioner for human rights to protect human rights and freedoms (apparatus)"
No. EuropeAid/137673/DD/ACT/UA

Activity 2.1.4. Developing new or improving the existing methodologies and procedures to carry out a monitoring of the observance of human rights, ensuring activities of the Ombudsperson in preventing such violations

Document	Guidelines and Checklist on Video Surveillance for Data Controllers of Public and Private Sector
Short description of the document	The Guidelines offer recommendations and suggest best practice on video surveillance. They are aimed at ensuring compliance with the provisions of the Law on the Legal Protection of Personal Data of Ukraine while at the same time enhancing the effectiveness and security of the systems and increase the trust within society. The Guidelines are addressed in particular to those who decide whether to install video-surveillance system and are responsible for proper operation (the data controllers) and, in addition, to suppliers and other contractors (usually acting as data processors) involved in the installation and operation of them.
Author	Dijana Šinkūnienė
Date	December 2017, Kyiv

GUIDELINES AND CHECKLIST

ON VIDEO SURVEILLANCE FOR DATA CONTROLLERS OF PUBLIC AND PRIVATE SECTOR

Table of content

1. INTRODUCTION

The use of video surveillance by public and private sector organizations has spread out in recent years. As technology has evolved, video surveillance is increasingly accessible to a large range of organizations. The use of video surveillance equipment is also influenced by decrease of prices. Security and crime control concerns are the most common motivating factors for the deployment of video surveillance cameras, however, the capabilities of the equipment, the wide range of collected data could be used in various ways that very often poses additional risks to privacy. Cameras are installed in public areas, in premises of public and private organizations (in government buildings, in stores, airports and banks, on streets and even in schools), apartment buildings. They are no longer a passive technology that only records and retains images, but is a proactive one that can be used to identify people of interest and keep detailed records regarding people's activities (for example, such as automatic number plate recognition cameras). The use of video surveillance cameras in this way raises additional concern as the technology is being used not solely to keep people and their property safe, but increasingly being used to track individuals and to collect evidence in order to take decisions related to particular person. As a rule, many of these devices have a capability that creates additional privacy risks – they capture not only image, but also sound data.

Equipment including night-vision cameras, time-lapse recorders, wireless pinhole cameras, surveillance vans, broadcast capable camera systems, facial recognition software, automatic number plate recognition software, unmanned aerial vehicles (drones) and body-worn video equipment are all becoming common surveillance tools. These Guidelines refer to any video surveillance technology that enables continuous or periodic recording (videotapes, photographs or digital images), or just on-line monitoring of different kind of areas, including any of aforementioned functionalities.

The Guidelines offer recommendations and suggest best practice while acknowledging that within the limits provided by personal data protection legislation each data controller has a margin of discretion on how to design its own system. The flexibility of Guidelines should ensure interpretation of personal data protection principles in a manner consistent with justified security needs or other legitimate objectives.

Following the guidance is often the most efficient way to comply with the law. The Guidelines are aimed at ensuring compliance with the provisions of the Law on the Legal Protection of Personal Data of Ukraine while at the same time enhancing the effectiveness and security of the systems and increase the trust within society.

The Guidelines are addressed in particular to those who decide whether to install video-surveillance system and are responsible for proper operation (the data controllers) and, in addition, to suppliers and other contractors (usually acting as data processors) involved in the installation and operation of them.

2. SCOPE OF APPLICATION

The specific features of the processing of personal information included in sound and image data have been expressly highlighted by Directive 95/46/EC (hereinafter referred to as "the Directive"), which refers to them expressly in several points.

The principles of data protection should apply to any information concerning an identified or identifiable natural person. Specificity and sensitivity of the processing of sound and image data concerning natural persons are highlighted in the recitals and the relevant articles of the Directive. Recital 14 underlines the importance of the ongoing development of techniques used to capture, transmit, manipulate, record, store or communicate sound and image data relating to natural persons, and clarifies that Directive should be applicable to processing involving such data. This means that more and more techniques and their functionalities appear which could cause unacceptable intrusiveness in person's private life. Following provisions of Article 2 (a) setting up a definition of personal data (any information relating to an identified or identifiable natural person ('data subject')) and those of recital 26, all the means likely reasonably to be used either by the data controller or by any other person aimed to establish the identity of the natural person should be taken into account.

On the other hand, development of the techniques gives more and more solutions how to render personal data anonymous in such a way that the data subject is no longer identifiable. Article 25 of the Regulation (EU) 2016/680 (hereinafter – General Data Protection Regulation) obliges the data controller to implement privacy by design principle which means that both at the time of the determination of the means for processing and at the time of the

processing itself, appropriate technical and organisational measures which are designed to implement data protection principles in an effective manner and to integrate the necessary safeguards into the processing shall be taken.

The principles of personal data protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable. In the context of video surveillance, it shall mean that collected data shall not contain any information (face image, voice, car number, home address, etc.) enabling direct or indirect identification of a particular person.

Personal data protection principles are not applicable to the personal data of deceased persons. However, if such kind of data are closely related to alive persons (for example, the data are used in order to characterize data subject by describing his/her relationship with deceased person), these data could be considered as personal data of that alive person. As regards information related to deceased persons, relevant provisions of civil law should also be taken into account.

Personal data protection principles do not apply to the processing of personal data carried out by a natural person in the course of a purely personal or household activity without connection to a professional or commercial occupation, therefore use of video surveillance systems for limited household purposes can be exempt from application of these Guidelines. Surveillance of private areas of other persons such as for example neighbours' gardens, entrance to their houses etc. may also be subject to civil law regulating privacy matters.

These Guidelines shall not be applicable to the covert surveillance activities carried out by competent public authorities empowered to ensure national security, as well as in the course of criminal intelligence which is regulated by Criminal Procedure Code of Ukraine.

The use of conventional cameras by the media for journalistic or for artistic purposes (news, film making etc.) are also not covered by these Guidelines.

3. COMPLIANCE WITH PERSONAL DATA PROTECTION PRINCIPLES

Personal information included in sound and image data collected by means of video surveillance concerns identified and/or identifiable persons. An individual moving in public or publicly accessible areas and premises may expect a lesser degree of privacy, but should not be deprived in full of his rights and freedoms, especially those related to his own private sphere and image. As it was mentioned before, personal data protection principles apply by also having regard to the importance of the developments of the techniques used to capture, manipulate and otherwise process personal data (for example, use of software applications based on facial recognition and enabling study and forecasting of the human behavior; techniques enabling dynamic-preventive surveillance, etc.).

Article 29 Data Protection Working Party in its Opinion WP 89[1] underlined that image and sound data relating to identified or identifiable natural persons is personal data even if the images are used within the framework of a closed-circuit system, without associating them with a person's particulars, and even though the data captured contain other information such as, for instance, car plate numbers or PIN numbers as acquired in connection with the surveillance of automatic cash dispensers, which enables indirect identification of a person. Moreover, in the Opinion WP 136 on the concept of personal data[2] it was underlined that: "In these cases, where the purpose of the processing implies the identification of individuals, it can be assumed that the controller or any other person involved have or will have the means "likely reasonably to be used" to identify the data subject. In fact, to argue that individuals are not identifiable, where the purpose of the processing is precisely to identify them, would be a sheer contradiction in terms. Therefore, the information should be considered as relating to identifiable individuals and the processing should be subject to data protection rules". This is particularly relevant in the context of video surveillance, when the purpose is to identify the persons appearing in the video images in all cases where such identification is deemed necessary by the controller. For this reason, such kind of video surveillance is to be considered as processing data about identifiable persons.

[1] Available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp89_en.pdf
[2] Available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf

The media used for the processing (e.g., fixed and/or mobile video systems such as portable video receivers, body warn cameras, unmanned aerial systems (drones), etc.), the technique used (cabled or fibre optic devices), the type of equipment (stationary, rotating, mobile), the features applying to image acquisition (e.g. continuous, or discontinuous – for example, when the image acquisition only occurs in case a speed limit is not respected), the communication tools used (e.g. the connection with a "centre" and/or the circulation of images to remote terminals, etc.) also does not play a crucial role.

Identifiability within the meaning of personal data protection legislation may also result from matching the data with information held by third parties, or else from the application, in the individual case, of specific techniques and/or devices.

The applicability of the personal data protection principles may be lifted for images that cannot be magnified or otherwise do not include information related to natural persons, as these images may be collected to identify objects, but not individuals (e.g. waste disposal areas, etc.), or equipment may be used to monitor various processes (e.g. motorway traffic, etc.).

As data captured using video surveillance equipment is personal data in most cases, the principles relating to processing of personal data set up in Article 6 of the Law on the Legal Protection of Personal Data of Ukraine as well as other provisions such as those regulating lawfulness of processing, including special categories of personal data, data subjects' rights, the safeguards applying in connection with automated individual decisions, security of processing operations, etc. shall be applicable.

3.1. PURPOSE LIMITATION PRINCIPLE

Before deciding to install a video surveillance system the data controller must first establish the purpose of the video-surveillance and must make sure that this purpose is legitimate. Following provisions of Article 6 of the Law on the Legal Protection of Personal Data of Ukraine, as well as Article 5 (1) (b) of the General Data Protection Regulation, personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a

manner that is incompatible with those purposes. Therefore, the purpose of video surveillance must be clear, specific and explicit. Vague, ambiguous, or simply too general descriptions, like for example „for better exercising of tasks conferred on the institution", „contributing to safety of the society" and similar are not sufficient. The data controller should bear in mind that **a broad definition of purpose does not justify collection and further use of data.**

Being specific about the purpose of the video surveillance can help the data controller to comply with the law, assess the necessity of such kind of personal data processing, ensure proportionality and transparency explaining why video surveillance is needed, follow national provisions related to notification and/or other obligations.

Further, it must be ensured that the data are not subsequently used for unforeseen purposes or disclosed to unforeseen recipients who might use them for additional, incompatible purposes. Incompatible purposes do not only include new purposes altogether unrelated to the initial purposes, but also all such purposes which would not have been reasonably expected by the individual under surveillance. For example, when it was announced to staff that a video-surveillance system is installed for security purposes, recordings should not be used to assess how well staff perform their job or whether they come to work on time. In some cases, e.g., on the request of staff representatives, it would be recommended to establish clearly the limitations on the use of the data.

Video surveillance in the workplace may be used only when because of the specifics of the work it is necessary to ensure security of persons, property or the public safety and in other cases when other means or measures are insufficient and/or inadequate for the achievement of the abovementioned purposes[3]. Goals such as managing productivity of workers, ensuring quality control, enforcing data controller's internal policies, providing evidence for dispute resolution and similar do not justify video surveillance of employees.

Taking into account technological development and especially capabilities given by video analytics, it is possible for an employer to monitor the worker's facial expressions by

[3] For example, airports, banks, areas of production in factories, etc.

automated means, to identify deviations from predefined movement patterns, etc. Article 29 Data Protection Working Party in its Opinion WP 249[4] underlined that: "This would be disproportionate to the rights and freedoms of employees, and therefore, generally unlawful. <…> There may be some fringe exceptions to this rule, but such scenarios cannot be used to invoke a general legitimation of the use of such technology".

It should be noted that the relevant purposes, together with other important privacy policy features, should be referred to in a document approved by the data controller. For the sake of transparency, the purposes of the processing must be communicated to the public on-the-spot in a summary form and in more detail, for example, via the public on-line version of the video surveillance policy.

3.2. LAWFULNESS OF PROCESSING

As for the lawfulness, it is necessary for the processing of personal data by means of video surveillance to be grounded on at least one of the conditions referred to in Article 11 or, in case of processing of special categories of personal data[5], in Article 7 of the Law on the Legal Protection of Personal Data of Ukraine. This might be data subject's consent, necessity for the performance of a contract to which the data subject is party, for compliance with a legal obligation to which the data controller is subject, for the protection of the data subject's vital interests, for the performance of a task carried out in the public interest or in the exercise of official authority, necessity for the purposes of the legitimate interests pursued by the controller or by a third party (balance of interests), etc.

It should be noted that in many cases data processing by video surveillance equipment is not regulated by specific legal acts. In such cases the data controller must carry out "balance of interests" test, which means that legitimate interests of the data controller or a third party must be measured against legitimate interest of the data subject, namely, his/her right to privacy and personal data protection. The following guidelines might serve in order to assess necessity of video surveillance and to weight before mentioned interests:

[4] Available at: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

[5] Data about racial or ethnic origin, political views, religious or other convictions, membership in political parties and trade unions, criminal record as well as if data relate to health or sexual life, biometric or genetic information is considered as special categories of personal data (see Article 7 (1) of the Law on the Legal Protection of Personal Data of Ukraine).

- Is the aim pursued quite serious and important in itself (for example, public safety, public order and protecting person's life, health, property and other rights and freedoms of persons)?
- Were the other ways or measures considered to achieve the aim pursued (for example, safety at work in many cases might be ensured by other means, while video records may serve only as evidence)?
- Are these other ways or measures insufficient and (or) inadequate for the achievement of the above-mentioned purposes (for example, the entity has a guard, but he/she cannot ensure safety of the territory outside the building at night – in such case video surveillance would contribute to achieving the established purpose)?
- Aren't the interests of the data controller overridden by the interests of the data subject (for example, in some premises, like toilets, changing-rooms, dormitories, doctor's cabinet the data subject reasonably expects absolute protection of privacy and therefore video surveillance would undermine human dignity).

Video surveillance should not be performed exclusively[6] on account of special categories of personal data, such as racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning health or sex life.

In case the video surveillance is regulated by specific legislation, the data processing carried out by the data controller should be in accordance with these provisions[7].

As regards obtaining the data subject's consent, the latter has to be unambiguous and based on clear-cut information. Consent has to be provided separately and specifically in connection with surveillance activities concerning particular premises[8].

[6] This means that video surveillance systems should not aim at capturing such data by zooming, indexing or otherwise processing the images. If there is an increased possibility that images revealing special categories of personal data will be captured, additional safeguards should be implemented (e.g. masking of images, live monitoring, etc.).

[7] For example, this might be the case of video surveillance in casino in many EU Member States.

[8] The data subject's consent might be a legal ground for video surveillance in case of installation of video surveillance in co-ownership (condominiums etc.). However, it should be noted that consent should not be used in employer-employee relationship.

As for the legitimate criteria where processing is necessary to protect vital interests of the data subject, the distance monitoring of patients in intensive care units might be an example. However, the video surveillance should really contribute for protecting vital interests, e.g. it should be born in mind that video equipment cannot replace human intervention which is usually needed in such cases.

In some cases, data controller is required to perform a task in the public interest or in the exercise of official authority possibly by complying with specific regulations – e.g. to detect road traffic offences or violent conduct in public high-crime areas.

It should be taken into account that preventing and controlling of crimes and offences is a task of particular state institutions (law enforcement agencies etc.) but not of every public or private entity or natural person. Therefore, the video surveillance for the before mentioned purposes (prevention of crimes, ensuring public order and similar) could be carried out only by authorities in charge to fulfill such functions under the law.

In other cases, the video surveillance serves for protecting property, ensuring safety etc., and is actually aimed at making available evidence of committed criminal offences.

3.3. THE PRINCIPLE OF PROPORTIONALITY AND DATA MINIMIZATION

Following Article 6 (3) of the Law on the Legal Protection of Personal Data of Ukraine, personal data shall be appropriate, adequate and non-excessive with regard to the purpose of their processing. In terms of Article 5 (1) (c) of the General Data Protection Regulation, this is referred as "data minimization" principle which first of all means that video surveillance equipment may only be deployed on a subsidiary basis, e.g. for purposes that really justify recourse to such measure. In other words, video surveillance systems may be installed if other prevention, protection and/or security measures, of physical and/or logical nature (e.g. armored doors, alarm systems, better and stronger lighting of streets at night etc.) requiring no image acquisition prove clearly insufficient and/or inapplicable with a view to the established legitimate purposes. **Alternative measure can be considered adequate unless it is not feasible or significantly less effective than video surveillance, or would involve disproportionate costs.**

It should be noted that mere availability of the technology at a low cost is not sufficient to justify the use of video surveillance system. The impact on the data subjects' legitimate interests and their fundamental rights shall be taken into account. With this regard he possibility to achieve the purposes without making recourse to personal data or by using really anonymous data should be assessed.

As for proper implementation of the principle of proportionality, the filming arrangements should be set up by having regard, in particular, to the following issues:

- **the area (territories, premises, parts of them) subject to video surveillance.** It should be noted that video surveillance in many cases is less privacy intrusive in outside territories in comparison to inside premises, as latter always poses risks to capture more personal data (for example, related to job performance, etc.). For this reason, the possibility to monitor only entrances to buildings should be assessed before having recourse to surveillance of premises;

- **number, location of cameras and the visual angle as related to the purposes sought.** If the video surveillance is necessary for monitoring outside territory of a private company, the cameras should not catch public places or areas belonging to other owners[9]. If the surveillance is performed by a public-sector body in a public place, the visual angle of cameras should not cover private territories or objects located nearby (private houses, or even entrances or windows of residential buildings). This is particularly important if zooming functions are implemented. Number of cameras is important as using too much of them increases likelihood that the information overload occurs and cameras will not be used efficiently;

- **the type of equipment used for filming,** i.e. whether fixed or mobile, as well as other functionalities, like for example cameras with sound recording or those equipped with

[9] Areas belonging to other owners could be monitored upon mutual agreement defining the role of everyone of them (e.g. responsibilities of data controller and data processor).

loudspeakers (so-called "talking CCTV"[10]) allowing to send alerts. Due to their intrusiveness, the use of sound recording and "talking CCTV" should be in principle avoided in both public and private sector. Exception might be using them as a back-up system for access control to premises outside working hours (as a video-phone to contact the remotely located security personnel to gain access), but not for exercising real time control over staff performing their job or those committing minor infringements in public places. Cameras with sound recording are also extremely privacy intrusive and therefore should not be used;

- **the use of webcams**[11] may give rise to specific data protection risks many of them being connected to the lack of control on who will view and use the images and for what purposes. The images can be easily recorded, copied, further distributed and used in any clearly undefined way by a multitude of recipients. When compared with the benefits of webcam use – which is often limited to pure "entertainment" – the increased risks that the images will be misused are in most cases not justified and therefore webcams should not be used;

- **resolution and image quality.** Settings ensuring appropriate image quality enabling to recognize facial images should be chosen. On the other hand, when identification of individuals is not necessary, the camera resolution and other factors should ensure that facial images shouldn't be recognizable;

- **continuous surveillance vs. fixing images when infringement occurs.** This might be the case if image acquisition only takes place if, for example, a speed limit is not respected[12] or in similar cases. As regards continuous surveillance, time periods of monitoring could also be important and therefore should be assessed, for example, for prevention of thefts it might be sufficient to switch on the cameras during the night and on weekends.

[10] "Talking CCTV" could be defined as video-surveillance configuration using loudspeakers in the area under surveillance and enabling the operators of the system to "talk" to the people being under surveillance.
[11] Webcam is a digital camera that transmits images, usually in real time, over the Internet for anyone who visits relevant webpage. Devices connected to the data controller's Intranet or otherwise transmitting images to the specific audience are also covered by these Guidelines.
[12] In this particular case the possibility of filming the relevant plates rather than the inside of vehicles should be considered.

- **the storage of the records vs. on-line monitoring.** In latter case the steps taken as a result of video surveillance (i.e. calling up surveillance staff, etc.) should be foreseen;

- **interconnection of video surveillance systems or facilitating identification of a person** by associating the images of the person's face with other information concerning his/her conduct and/or activities, for example in the case of the association between images and data related to the activities performed by clients of a company at an easily identifiable time. Interconnection of video surveillance systems operated by different public bodies or matching images with personal data processed in state owned data bases in many cases would raise the issue of incompatibility of data processing purposes and go beyond the provisions of Article 6 of the Law on the Legal Protection of Personal Data of Ukraine. Such kind of processing should be carefully assessed and regulated by appropriate legal act.

All traits mentioned above should be assessed before purchasing video surveillance system in order to decide on the appropriate filming arrangements complying with the proportionality principle. It should be noted that such kind of assessment would not only ensure protection of data subjects' rights but could also contribute to the proper use of the resources of the data controller (e.g. preventing from wasting finances on the equipment with excessive functionalities).

3.4. STORAGE LIMITATION

As regards retention of the recordings, first of all possibility of live monitoring must be considered. If recording is necessary, decision should be taken on retention period. It should be noted that the retention period has to be quite short, in line with the specific purposes of video surveillance and taking into account specific features of the individual case. For example, in the case of observance by the personnel of health care center of very seriously ill patients only live monitoring is allowed, while for purposes of protection of private premises recording of images could be justified.

The period of time for which the recordings will be retained shall be set up in the video surveillance policy or other internal document approved by the data controller. After the lapse of this period the recordings must be erased. For the sake of compliance, the process of erasure should be automated. Once the media is no longer useable it must be safely destroyed in such a manner that the remaining data on it would be permanently and irreversibly deleted (e.g. via shredding or other equivalent means). An exception to this rule would be the case when recordings are necessary to further investigate the incident or use the recordings as evidence. For these purposes the relevant footage may be retained longer than defined retention periods, but only for as long as it is necessary for these purposes.

Retention period should be defined taking into account time limit sufficient for responsible personnel to decide whether to retain any footage for longer period in order to further investigate incident or to use recordings as evidence. It would be strongly recommended to keep register of recordings stored beyond the retention period, indicating at least the date and time of the footage, a short description of the incident and the reason why the footage is needed. The expected date of the review of the necessity of such longer retention should be foreseen.

Usually recordings could be kept from several ours to one week. In exceptional cases this time period might be one month. Length of the storage might also be influenced by the area under video surveillance and the type of personal data collected. For example, if the video surveillance covers outside area near the entrance to the building and there is no possibility to avoid surveillance of passers-by, or if records could reveal special categories of data[13], the time limits of storage must be shortened.

[13] This might be the case when filming demonstrations, entrances to religious, medical care buildings, etc. It should be noted that video surveillance of such kind of areas first of all must comply with purpose limitation, lawfulness and adequacy principles. Live monitoring also must be considered in these cases.

4. DATA SUBJECT'S RIGHTS

The peculiar features of the personal data collected by means of video surveillance do not rule out exercise by data subjects of the rights referred to them neither in EU legislation (Articles 13 and 14 of the Directive and Articles 12 – 22 of the General Data Protection Regulation) nor the Law on the Legal Protection of Personal Data of Ukraine. Indeed, the data subject has a right to object at any time to the processing of data relating to him on compelling legitimate grounds relating to his particular situation.

Despite the usually short retention period of the images, the data subject retains the right of access to personal data that make him/her identifiable. However, none of the rights of the data subject could oblige the data controller to establish longer periods of storage of the video records than those necessary with regard to the legitimate and defined purposes. The rights of third parties also should be taken into account.

However, it should be noted that any limitations grounded on the disproportionate efforts to be made for retrieving the images (for example, in terms of researches, costs and resources), should be laid down exclusively by primary legislation (see Article 13(1) of the Directive, Article 23 (1) of General Data Protection Regulation, Article 25 (1) of the Law on the Legal Protection of Personal Data of Ukraine).

4.1. RIGHT TO BE INFORMED

Taking into account the scope of these Guidelines, covert surveillance should not take place, therefore relevant information foreseen in Article 8 (2) (1) of the Law on the Legal Protection of Personal Data of Ukraine should be provided to the public. Taking into account peculiarities of video surveillance, it should be done in an effective and comprehensive manner. For this reason, it would be advisable to use two methods[14]:

- **To provide on-the-spot notices** containing essential information about the processing. This information should contain at least the fact that video surveillance takes

[14] These two methods are suggested in the European Data Protection Supervisor Video-Surveillance Guidelines (available at: https://edps.europa.eu/sites/edp/files/publication/10-03-17_video-surveillance_guidelines_en.pdf).

place and the requisites (title/name, surname[15] (if the data controller is a natural person) and effective contact details (address, phone number, e-mail, etc.) where the data subject could get additional information. Possible templates of notices are provided in Annex 1 to these Guidelines.

It is very important that the contact details of the data controller provided in on-the-spot notice would be effective, e.g. that response to the data subject's request for additional information should be given promptly and clearly.

The notices should be visible and positioned at a reasonable distance from the monitored places. Information may be provided in a summary fashion, also it may include symbols. The format of the information should be adjusted to the individual location, but this does not mean that a notice must be placed next to every single camera. However, if any cameras are placed at a location where there could be heightened expectation of privacy or where the cameras would otherwise be unexpected, an additional on-the-spot notice should be provided prior to the entrance of the monitored premises.

As regards monitoring of public areas (streets, squares, etc.) for public safety reasons by the authorized public authorities (e.g. police), notices on the roads before entering a town are not sufficient as they could not specify particular areas of video surveillance. For this reason, they might be useful only as auxiliary measure.

- **Detailed data protection notice** posted on the data controller's Internet site or made otherwise available for those who wish to get more information regarding video surveillance. Placing relevant part of the document regulating the data processing procedure (video surveillance policy) online instead of preparing a separate data protection notice might be well compatible with the purpose to provide data subjects with detailed information.

[15] Name and surname of the natural person should appear on the notice when he/she acts as the data controller in the course of the activity related to business or profession (attorney, etc.). Name and surname of the natural person who is merely responsible for the protection of personal data in the entity should not be made public.

The two above mentioned methods (on-the-spot notice and detailed data protection notice) can be supplemented by others (printed hard copies of the detailed notice, information provided by phone or e-mail, provision of detailed information on the Intranet, leaflets, etc.). However, none of these other methods could replace on-the-spot notice.

Staff at the data controller must be trained on the data protection and video surveillance practices and must be able to make copies of the detailed data protection notice (video surveillance policy) instantly available upon request of the data subject. They must also be able to tell data subject whom to contact with additional questions or in order to access their data.

4.2. RIGHT OF ACCESS

Taking into account Article 12 of the Directive, Article 15 of General Data Protection Regulation, Article 8 (2) of the Law on the Legal Protection of Personal Data of Ukraine, the data subject has a right of access to his/her personal data.

When exercising this right, access needs to be given to the recordings by allowing the individual to view them or by providing a copy to him/her. The rights of third parties present on the same recordings need to be carefully considered and protected. This would require image-editing such as masking or scrambling. Otherwise, the legal ground for disclosure of personal data of third parties appearing on the record is required (consent or other). Protection of the rights of third parties, however, should not be used as an excuse to prevent legitimate claims of access by individuals.

The data subject asking for access shall provide proof of identity, photo, and, in order to facilitate examination of the request, might be asked to specify the time and location of the

recording. Other conditions specified in Articles 16 and 17 of the Law on the Legal Protection of Personal Data of Ukraine shall also be fulfilled.

Following Article 19 (1) of the Law on the Legal Protection of Personal Data of Ukraine, access of a data subject to data on himself/herself shall be free of charge.

If access to personal data is refused, reasons for refusal, as well information on the right of appeal to the Ukrainian Parliament Commissioner for Human Rights or to the court shall be provided to data subject.

5. SECURITY MEASURES APPLICABLE TO DATA PROCESSING

Following Article 17 of the Directive, Article 32 of General Data Protection Regulation, Article 24 of the Law on the Legal Protection of Personal Data of Ukraine, the data controller and data processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed. This obligation is applicable to full extent in the video surveillance context.

It would be suggested, among others, to take the following measures:

- determining the processing procedure of personal data (video surveillance policy);
- providing trainings on personal data protection to the staff involved in personal data processing;
- to implement physical security measures (protected premises, including those hosting the servers in which recorded images are stored; perimeter of the IT infrastructure protected by network firewall, etc.);
- to take measures of administrative nature (signing confidentiality agreements with internal and external staff[16] having access to video surveillance system, etc.);
- to manage access rights of users (access rights should be granted by the system administrator in accordance with defined procedure on strictly necessary basis only to those for whom are necessary in order to carry out their jobs; keeping up-to-date list of all persons having access to the video surveillance system, etc.).

[16] External staff also include those maintaining functioning of the system, providing technical assistance, etc.

5.1. DEFINING THE DATA PROCESSING PROCEDURE (VIDEO SURVEILLANCE POLICY)

Following Typical procedure for processing of personal data approved by Decree of the Ukrainian Parliament Commissioner for Human Rights of 8 January 2014 №1/02-14 (hereinafter – the Procedure), the data controllers and data processors shall determine the processing procedure of personal data, taking into account the specifics of personal data in various fields, according to requirements defined by the Law on the Legal Protection of Personal Data of Ukraine and the Procedure. Taking into account the content of the Article 2 of the Procedure, as well as taking into consideration the peculiarities of video surveillance, the following aspects should be included in the data processing procedure approved by the data controller and made publicly available (posting it on internet site or making it otherwise available to data subject) **in order to provide detailed data protection notice as referred in Chapter 4.1 of these Guidelines**[17]:

- identity of the controller (e.g. title of the company, state institution, name and surname of natural person acting as data controller);
- the legal basis of video-surveillance;
- description of the coverage of the video-surveillance system by indicating territories and premises;
- the purpose of video-surveillance;
- who has access to the video-surveillance footage, and to whom the images may be disclosed (it would also be suggested to clearly specify any limitations on the permissible uses);
- how the information is protected and safeguarded;
- information regarding on-line monitoring and, in case the recording is being made, how long the data are kept;
- how data subjects can implement their rights (right of access, as well as how to verify, modify or delete information related to them), as well as contact information for further questions;
- the right to recourse to the Parliament Commissioner for Human Rights.

[17] In such case there would be no need to draft and post a separate on-line data protection notice.

In addition, the data processing procedure (video surveillance policy) should also include:

- number of cameras, their location[18] and visual angle[19];
- any special capabilities of video surveillance system (e.g. zoom function, facial recognition, night-vision features, etc.);
- time periods when video surveillance shall be in effect;
- procedure of periodic review of the necessity of video surveillance[20];
- procedure of erasure of data after expiration of storage period;
- procedure related to providing information to data subjects (provision of information on-the-spot, etc.) and implementing other rights;
- information regarding notification of processing to the Parliament Commissioner for Human Rights in accordance with Article 9 of the Law on the Legal Protection of Personal Data of Ukraine;
- explicit confirmation as to the compliance with the Law on the Legal Protection of Personal Data of Ukraine[21];
- procedure of getting access to personal data for persons engaged in the processing;
- procedure of granting access for third parties;
- outsourcing of data processing operations;
- procedure relating to keeping a register of transfers and disclosures of data[22];
- procedure relating to an internal analysis of the security risks;
- privacy-friendly technological solutions[23];
- security measures used to protect video surveillance system (use of secure communication channels, protection of physical access to the control room, location of monitors, logging system enabling to determine who, where and when accessed the system, etc.);

[18] It would be advisable to attach detailed map with exact camera location.
[19] It is important to indicate visual angle of camera when the target of video surveillance is particular item, for example, cash desk.
[20] The purpose of such periodic reviews is to check whether video surveillance is still the best solution with regard to problem the data controller is trying to address.
[21] Audit report, if any, should be provided as attachment.
[22] This register should include at least the date of the request, the requesting party, the reason of the request and the reason for granting it, whether a copy of data was transferred.
[23] For example, encryption of data, masking of images in order to eliminate surveillance of areas irrelevant to target of surveillance, etc.

- other relevant information (e.g. providing explanation why other measures appear to be inappropriate or insufficient in a particular case and why recourse has been made to video surveillance, etc.).

In order to demonstrate compliance, it would be strongly recommended to carry out audit prior to the launch of the video-surveillance system as well as periodic audits and document their results in audit reports.

5.2. DATA PROCESSORS AND THIRD PARTIES

The private entity or public-sector body responsible for data processing (the data controller) might outsource its video surveillance operations, however, it should be noted that it will remain liable as the data controller. The obligations of the data processor must be clarified in writing and in a legally binding manner. This usually means that there must be a written contract in place between the data controller and the outsourced company. The contract, as well as the tender specifications (this is especially important for data controllers of public sector) should foresee that the contractor should comply with the provisions of the Law on the Legal Protection of Personal Data of Ukraine and secondary legislation, data controller's video surveillance policy, follow any instructions of the data controller regarding data processing and security, as well as any advice of the Parliament Commissioner for Human Rights. The obligations of the contacted company related to security, confidentiality, training of staff on data protection must be clearly stated. Any direct or indirect subcontractor must be bound in the same way (in written) and by the same obligations as the direct contractor.

Sometimes video-surveillance is not carried out by the private entity or public-sector body or a contractor on their behalf, but rather by the landlord from whom the premises are leased. In some cases, there may be a complex contractual system involving several leases and subleases, and/or several contractors and subcontractors and the contractual influence on the operator of the video-surveillance system might be complicated. However, it would be recommended to negotiate the issues related to video surveillance before entering into contractual obligations. There might be two main scenarios distinguished:

- video surveillance carried out outside the buildings often can be justified by the interest of landlord (for example, to ensure security of property), therefore a landlord will act as data controller[24];
- as regards video surveillance carried out inside the buildings (in the premises used exceptionally by particular leaseholder), in most cases the landlord would not have legitimate interest for carrying out video surveillance. Therefore, only the leaseholder could be considered as the data controller with regard to video surveillance[25]. The landlord and company outsourced by him, if any, would act as the data processors of leaseholder.

6. FINAL PROVISIONS

The data controllers should take steps in order to ensure compliance with these Guidelines. As regards compliance for already existing systems, the data controllers should verify their existing practices, identify what further steps are necessary to ensure full compliance, and implement all necessary measures. The Checklist on Video Surveillance provided in Annex 2 to these Guidelines is intended to help data controllers to comply with provisions of the Guidelines as regards systems already in place as well as when introducing new ones.

---

[24] However, if video surveillance is also necessary for purposes of leaseholder (for example, in order to ensure security of cars parked beside the buildings), both of them could be considered as joint controllers and their obligations regarding video surveillance should be described in contract or in other written document.
[25] On the condition that video surveillance is in line with personal data protection principles.

Annex 1

POSSIBLE TEMPLATES OF ON-THE-SPOT NOTICES

Example 1

VIDEOSURVEILLANCE IS CARRIED OUT FOR PURPOSES OF SECURITY

Company „TITLE“
Phone: +00 000 0000
E-mail: company@info.com

Example 2

PREMISES ARE UNDER VIDEO SURVEILLANCE

Name Surname
Phone: +00 000 0000
e-mail: name@mail.com

Annex 2

CHECKLIST ON VIDEO SURVEILLANCE

..../..../.....
(date)

_____
(Title/name, surname of data controller)

No.	Issue	Yes	No	Remarks*
	Compliance with personal data protection principles			
1.	The problem to be addressed by video surveillance is clearly defined.	☐	☐	
2.	The aim pursued by video surveillance is serious and important (public safety, protecting person's life, property, etc.).	☐	☐	
3.	Before having recourse to video surveillance, other ways and/or measures were considered to achieve the aim pursued.	☐	☐	
4.	The interests of the data controller are not overridden by the interests (expectation of privacy) of the data subject.	☐	☐	
5.	Video surveillance is not carried out in premises with higher expectations of privacy (toilets, changing rooms, dormitories, leisure rooms, doctor's cabinet, etc.).	☐	☐	
6.	Video surveillance is not performed exclusively on account of special categories of personal data (racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning health or sex life).	☐	☐	
7.	Video surveillance is considered to be the best solution in this particular case.	☐	☐	
8.	The purpose of video surveillance is clear, specific and explicit.	☐	☐	
9.	Video surveillance has a legal ground referred to in Article 11 or Article 7 of the Law on the Legal	☐	☐	

	Protection of Personal Data of Ukraine.			
10.	Correspondence of functionalities of the equipment to the personal data protection principles have been evaluated before purchasing it.	☐	☐	
11.	The filming arrangements have been set up taking into account:			
11.1.	territories, premises, parts of them subject to video surveillance;	☐	☐	
11.2.	number, location, visual angle of cameras;	☐	☐	
11.3.	resolution and image quality.	☐	☐	
12.	Possibility of live monitoring and/or discontinuous surveillance has been evaluated and appropriate decisions have been taken.	☐	☐	
13.	Retention period of recordings corresponds to the purposes of video surveillance and does not exceed one month.	☐	☐	
Data subject's rights				
14.	On-the-spot notices informing about video-surveillance are visible and positioned at a reasonable distance from the monitored places.	☐	☐	
15.	On-the-spot notices contain title/name, surname of the data controller and effective contact details.	☐	☐	
16.	Detailed data protection notice is posted on the data controller's website and/or is available upon request of the data subject.	☐	☐	
17.	Right of access to video records is implemented upon providing proof of identity, including photo.	☐	☐	
18.	Access to video records is given by allowing the individual to view them or by providing a copy.	☐	☐	
19.	When granting access to the data subject, rights of third parties appearing on the video record are protected.	☐	☐	
20.	Video records to data subjects are provided free of charge.	☐	☐	
Security measures applicable to data processing				

21.	The processing procedure of personal data (video surveillance policy) is determined.	☐	☐	
22.	Trainings on personal data protection are regularly provided to the staff involved in personal data processing.	☐	☐	
23.	Physical security measures (protected premises, including those hosting the servers in which recorded images are stored; perimeter of the IT infrastructure protected by network firewall, etc.) have been implemented.	☐	☐	
24.	Measures of administrative nature (signing confidentiality agreements with internal and external staff having access to video surveillance system, etc.) are in place.	☐	☐	
25.	Access rights of users are managed.	☐	☐	
26.	Other security measures (encryption, etc.) were taken following internal analysis of the security risks.	☐	☐	
27.	The obligations of a company outsourced for data processing (data processor) are set up in a legally binding manner (in a written contract, etc.)	☐	☐	

* In the column „Remarks“ it is advisable to provide information relating to particular situation, e.g., if the checklist is filled in with regard to video surveillance system already in place and some inconsistency is detected, the time limit for making corrections should be indicated; if some issues are not pertinent (for example, there is no outsourcing of data processing operations), this also should be marked; any additional explanations also could be provided there.

Checklist has been filled in by:

_____

(name, surname, job title)