úřad pro ochranu
osobních údajů
the office for personal
data protection

The Office for Personal Data Protection

Operation of Camera Monitoring Systems
Methodology for the Fulfillment of the Basic Obligations Imposed by the Personal Data Protection Act

Contents

Introduction

The presented methodology is to facilitate camera monitoring system operators (i.e., controllers or processors) with setting up and operating camera monitoring systems to ensure that such set-up and operation are carried out in compliance with Act No. 101/2000 Coll., on protection of personal data and on amendments to certain acts, as amended, by using certain defined procedures and templates. This guideline is to serve as a general reference only; the Office for Personal Data Protection provides consultation for more complicated issues.

Generally speaking, camera monitoring systems are most often introduced to provide protection to property and security to individuals. Future operators, however, often do not realize that camera monitoring systems are not the only effective means to protect property and people. In a host of cases, camera monitoring systems compensate for shortcomings in mechanical and electronic security. Furthermore, future camera monitoring system operators often fail to sufficiently assess the actual usability of data obtained by camera monitoring systems, i.e., the actual possibility of fulfilling the processing purpose itself.

1. Operation of Camera Monitoring Systems

Operation of a camera monitoring system is deemed to be the processing of personal data, provided that in addition to camera monitoring,[1]

- recordings (video or audio[2]) are made
- the purpose of making recordings is to use the recordings to identify (directly or indirectly) natural persons in connection with certain actions carried out by them.[3]

[1] *For the purposes hereof, camera monitoring shall mean use of available technology to generate/record images, broadcast images, and display images or images with audio (e.g., CCTV, trail cams, webcams, etc.).*

[2] *If an audio recording is made along with a video recording, an assessment should be made as to whether such recording is made in compliance with the purpose of processing and is truly necessary for fulfilling the purpose of processing [Section 5(1)(d) of Act No. 101/2000 Coll.]. In the vast majority of cases, this is not the case (video recordings are sufficient in most cases to prove a certain event). Making audio recordings (together with video recordings) represents a gross infringement of the privacy of the monitored individuals, and the scope of the processed data should* thus *be limited to making video recordings only.*

[3] A *simple camera recording, processed and used in the usual way, shall not be deemed the processing of sensitive data. In principle, it is the visual identification of persons in connection with their certain actions. The controller, for example, identifies a recording showing that a crime is being committed by a certain person, regardless of such person's nationality, race, ethnicity, religion, state of health or such person's biometric characteristics. Processing sensitive data would occur if certain biometric characteristics of the subject concerned (facial characteristics/prominent features or use of facial recognition system, biometric characteristics of gait, etc.) were stored during recording.*

Operating a camera monitoring and recording system[4] (and thus even personal data processing) is possible based on a number of reasons:

- **If it is necessary to protect the rights and the legally protected interests of the controller or other entity** - this is the most common reason for operating a camera monitoring and recording system, typically to protect property. If the camera monitoring system is operated based on this legal reason, it is necessary to pay attention to not infringe excessively on the monitored individuals' right to privacy [Section 5(2)(e) and Section 10 of Act No. 101/2000 Coll.].
- **If the processing is necessary for the controller to fulfill legal obligations** - especially as part of fulfilling tasks stipulated by the law (e.g., Act No. 273/2008 Coll., on the Police of the Czech Republic, as amended; Act No. 553/1991 Coll., on the municipal police, as amended; Act No.412/2005 Coll., on protection of confidential information and security capacity, as amended, etc.[5]).
- **Based on the data subjects' consent[6] -** only in limited cases where it is possible to define the group of individuals to be monitored – for more information see, e.g. Standpoint of the Office for Personal Data Protection No. 1/2008 on Placement of Camera Systems in Residential Buildings and the Response and Recommendations of the Personal Data Protection Office on the Possibility of Installing Camera Monitoring Systems in Schools, available on the Office's website (see Chapter 5 below for more details on consent).

2. Notification Duty

1. Operation of a camera monitoring and recording system is considered to be personal data processing, which should be reported to the Office for Personal Data Protection in accordance with the notification duty under Section 16 of Act No. 101/2000 Coll.
2. To fulfill the notification/registration duty, it is possible to make use of an electronic form to submit the notification of processing (change of processing) of personal data pursuant to Section 16 of Act No. 101/2000 Coll. (the "form"), which is available on the website of the Office for Personal Data Protection, www.uoou.cz (in the Register column), where more detailed information on fulfilling the notification duty is provided.

---

[4] *In practice, monitoring-only camera monitoring systems (i.e., no recording) are used only rarely. Connecting the recording function to a camera monitoring system, or disconnecting it, is a relatively simple matter. However, the difference between the two options is significant from the perspective of the Personal Data Protection Act.*

[5] *Compare list of laws - see Chapter 1, page 4, on exemptions to the notification duty based on a special law.*

[6] ***Due to the frequency that camera monitoring systems appear during working hours at employer's premises, which are an employee's place of work, it is necessary to apply on top of the provisions of Act No. 101/2000 Coll. specific provisions of Act No. 262/2006 Coll., the Labor Code, particularly Section 316,*** *which only allow an employer to monitor an employee and otherwise infringe on his/her privacy for serious reasons consisting in the specific nature of the employer's business. If no such reason exists, the employer may not undertake monitoring, even if an employee consents to being monitored. This conclusion is based on the fact that the application of Section 316(2) of the Labor Code is mandatory and may not be circumvented even if the contractual parties agree to do so.*

3. In point 7 of the form (Description of the method of processing personal data), once the field "by camera monitoring systems - by processor" or "by camera monitoring systems - by own employees" is checked, an additional form appears with questions focused directly on processing using camera monitoring systems.

4. The addresses of the locations of cameras, addresses of the locations where recordings are stored and the addresses of the locations where the recordings are processed are deemed the locations where processing takes place under point 8 of the form, provided these addresses differ from the registered office of the controller/notifying party.

5. It is necessary to append the following annexes (if they exist) to the form:

   a) Copy of a power of attorney (does not have to be verified by a notary) if a different entity is representing the notifying party

   b) Lists of processing locations, provided such lists did not fit in point 8 of the form[7].

6. The Office for Personal Data Protection has 30 days to register the personal data processing notification in the register. The controller is authorized to begin processing personal data at the moment that the notification is registered in the register. The Office recommends that the applicant check that the registration has been carried out successfully on www.uoou.cz/Registr. A search can be conducted using the notifying party's name, ID No. or registration number - we recommend using only one identifier (preferably ID No.); the greater the number of identifiers, the greater the possibility of error.

7. The Office for Personal Data Protection issues the certificate of registration in the personal data processing register (registration) only at the controller's/notifying party's request.[8]

However, there are cases of personal data processing using camera monitoring systems to which the notification duty does not apply. These include the following:

1. Operating a camera monitoring and recording system for personal needs occurs if a natural person/citizen decides to protect his/her property by monitoring his/her private property, building, flat, including entrance, private parking spot, etc. The act does not apply to such processing [see Section 3(3) of Act No. 101/2000 Coll.], and, therefore, it is not necessary to submit a notification of personal data processing. In such cases, it is necessary, however, to assess whether the camera system will be operated at variance with other legal regulations. Personal data processing using camera monitoring systems has to be carried out in a way

[7] *Copies of the data subject's approval to have his/her personal data processed, security guidelines, camera monitoring system guidelines, and camera shots are often part of the notification, although they need not be appended. If doubts arise in the registration proceedings that the notification does not contain sufficient information to allow for the notification to be assessed, the Office for Personal Data Protection shall send the notifying party a request to supplement the notification and, in such request, specify the information and documents required.*

[8] *The registration proceedings under Section 16 of Act No. 101/2000 Coll. are not permit proceedings, and the issued certificate only proves that the controller fulfilled his statutory obligation to notify the Office for Personal Data Protection of the intended processing, and, at the same time, that he is registered in the register maintained by the Office for Personal Data Protection.*

that does not infringe on the privacy of other individuals (for more details, see Sections 12 and 13 of Act No. 40/1964 Coll., the Civil Code, as amended).

2. Operating a camera monitoring and recording system, the use of which is required by a special law or which is necessary to exercise the rights and obligations ensuing from a special law (for more details see Section 18 of Act No. 101/2000 Coll.). Examples of such special laws are as follows:

- Act No. 273/2008 Coll., on the Police of the Czech Republic, as amended
- Act No. 553/1991 Coll., on the municipal police, as amended
- Act No. 412/2005 Coll., on protection of confidential information and on security capacity, as amended
- Act No. 202/1990 Coll., on lotteries and other similar games, as amended
- Act No. 59/2002 Coll., on the prevention of serious accidents, as amended
- Act No. 18/1997 Coll., on peaceful utilization of nuclear energy and ionizing radiation and on amendments to certain acts, as amended
- Act No. 109/2002 Coll., on the provision of institutional education or protective education at school facilities and on preventative educational care at school facilities and on amendments to certain acts
- Act No. 129/2008 Coll., on enforcement of protective detention and on amendment to certain acts, as amended
- Act No. 326/1999 Coll., on the residence of foreign nationals in the Czech Republic and on amendments to certain acts, as amended
- Act No. 555/1992 Coll., on the prison service and the judicial guard of the Czech Republic, as amended
- Act No. 17/2012 Coll., on customs administration

3. Operating a camera monitoring system in the on-line/no recording regime.[9] Such operation of the camera system is not considered to be personal data processing in accordance with Act No. 101/2000 Coll., as it lacks certain characteristics of data processing, such as collection of personal data, storage of personal data, retrieval, etc. [Section 4(e) of Act No. 101/2000 Coll.] Nevertheless, even in such cases, the application of other legal regulations is not precluded (e.g., the Labor Code and Civil Code).

[9] *The various cameras of the camera operating system that are operated under the on-line/no recording regime need not be listed in the personal data processing notification under Section 16.*

3. Camera Monitoring System Documentation

A camera monitoring and recording system represents a special way of processing personal data and requires that it be documented in a special way. The following are the specific documents required:

- Documents drawn up in connection with the camera monitoring system layout and design:
    - Analysis of the security options for the monitored subject (i.e., buildings, facilities, persons), including an analysis of infringement of privacy, selection of option
    - Risk analysis
    - Project documents
    - Documents concerning the adopted technical and organizational measures (for more details see chapter 4)
    - Contractual documentation
    - Regulations (guidelines) for operating the camera system (optional).

- Document showing that consent was granted by the data subjects (natural persons/citizens) whose personal data is to be processed or by their statutory representatives (this concerns only a limited number of cases).[10]

- Documents drawn up in connection with operating the camera monitoring system:
    - Information signs at the monitored premises (see Chapter 6 below)
    - Detailed information that is provided to the data subjects (natural persons/citizens) on personal data processing as additional information to the signs designating which premises are being monitored [for more details see Section 11(1) of Act No. 101/2000 Coll.]
    - Documents pertaining to own operation and provision of personal data – information about who had access to the recordings, to whom they were provided and based on what authorization, information about unusual operational events, etc. (e.g., the operation journal, handover protocols).

[10] *See Chapter 4 for the consent template.*

4. Documentation Regarding Adopted Technical and Organizational Measures

If a camera system is used, it is necessary to undertake the following:

- Operation of a camera monitoring system needs to be preceded by an analysis of the various security options for the monitored subject; this analysis also includes an assessment of how to minimize infringement on privacy (for each option, an analysis and comparison of conflicts between opposing rights – whether the protection of a certain right takes precedence over the protection of privacy and private or family life; analysis of which security option is the most suitable for the monitored subject; analysis whether the respective option is able to fulfill the required purposes)[11]
- In the event that a camera monitoring and recording system was chosen based on an analysis of the security options for the monitored subject and this leads to the processing of personal data, it is necessary to further analyze the potential threats and propose the implementation of (technical and organizational) measures to eliminate such threats or to mitigate them to the maximum extent. The controller or processor of personal data shall document the (technical and organizational) measures (for more details see Section 13 of Act No. 101/2000 Coll.)
- Content of the documentation related to adopted technical and organizational measures:

1. **Identification of a camera monitoring system and its description**
   - Who is the controller
   - Who is the processor/operator (if one exists) authorized by the controller
   - Who is the designer and who is the supplier of the camera monitoring system
   - Where the camera monitoring system is located (address)
   - Number of installed cameras
   - Description of the range of the cameras and their operating regimes
   - Description of the technical solution (what kind of cameras, recording equipment, wiring, etc.)
   - Description of the training provided to the operating personnel and the arrangements made for maintaining the camera monitoring system.
2. **Description of technical and organizational measures** (*provide a more detailed technical description of each implemented measure*):
   Generally speaking, when processing personal data through a camera monitoring system, four types of threats can be defined:

a) Unauthorized access to the various components of the camera monitoring system

To the cameras

Examples of technical and organizational measures: placement outside the reach of persons moving about in the monitored premises, cameras used to check one another, camera security covers, etc.

[11] *The conducted analysis may prevent unnecessary expenditures related to the installation of camera monitoring systems, complaints from data subjects and even possible fines from the Office for Personal Data Protection should it be proven that the obligations set out in the Personal Data Protection Act have been breached.*

To the wiring

Examples of technical and organizational measures: wires running in protective guards, in sheathing, under plaster, cables ending in lockable distributor boards, camera monitoring system wiring separated from other networks, etc.

To recording equipment, PC

Examples of technical and organizational measures: placement in lockable buildings, lockable rooms, lockable equipment, barred windows, permanent security guard, restricted number of persons with access - record of keys, access based on cards/chips etc., movement sensors, access to room only under supervision or in the presence of more than one person, record of access to room, etc.

b) Unauthorized access to camera records (access by unauthorized persons)

Examples of technical and organizational measures: restricted access to building/room, user access procedure (login name, password, pin, etc.), data carriers part of recording equipment (data is not stored externally, outside recording equipment), record encryption, system for recording access to records and creation of copies of records, secure deletion/destruction of data carriers, separation of camera monitoring system from data networks, etc.

c) Unauthorized reading, copying, transmission, modification and deletion of camera recordings

Examples of technical and organizational measures: user access procedures (login name, password, PIN etc.), determining the role of user (for reading, for copying), data carriers part of recording equipment, antivirus SW, secure deletion/destruction of data, system records access to recordings and creation of copies of recordings, separation of camera system form data networks, records are created in the operational journal or in the protocols on handover of records to authorized persons, presence of authorized persons only when monitoring the recording or when making copies of recordings, training of operating personnel, arrangements for servicing the equipment, safety regulations, designation of administrator and/or security system administrator, etc.

d) Natural events – destruction of camera system including data (floods, fire, lighting strike, etc.)

In the case of most camera monitoring systems, this is a residual risk, i.e., a hazard that need not be eliminated or restricted in a special way.

3. **Verification of the functionality of technical and organizational measures**

Description of verifications of functionality of technical and organizational measures (frequency, who will perform the verifications and in what way, method of taking into account the results and recommendations of verifications).

5. Consent to Processing Personal Data via a Camera Monitoring System[12]

The following text only deals with the issue of consent to personal data processing, provided that personal data is processed based on such consent [for more details on legal regulations, see also Section 4(n) and Section 5(4) of Act No. 101/2000 Coll. and Standpoint of the Office for Personal Data Protection No. 2/2008].

1. Granting of consent only pertains to data subjects that are present in the monitored building/premises on a regular basis (e.g., pupils, students, and residents) and where processing in not possible based on an exemption from consent under Section 5(2)(a) to (g) of Act 101/2000 Coll.
2. Statutory representatives (legal guardians) provide consent on behalf of minors or legally incompetent individuals (consent from a legal guardian is recommended for minors up to the age of 15 years; from this age, it is assumed that the data subject is able to assess the scope and degree of the infringement of privacy and is thus able to provide consent with personal data processing him/herself).
3. On the other hand, consent is not required from data subjects that are visitors, suppliers (including postal service workers) or other persons entering the monitored building/premises by chance/for a short period of time/irregularly.
4. Consent has to be granted by the data subject or his/her statutory representative freely, consciously and in an informed manner (for example, consent should not be part of documents related to the conclusion of other relationships).
5. The controller has to be able to present valid consent from data subjects for the entire period that personal data is processed.
6. When granting consent, the data subject or his/her statutory representative has to be informed about the following:
   - Purpose of the processing of personal data
   - Extent of the personal data processing, i.e., particularly the location of the various cameras with a description of the premises being monitored and the regime in which the cameras are operated
   - Controller of the personal data
   - Period of time for which the consent is being granted
   - Who will be processing the personal data (the processor) and how
   - Who may be given access to the personal data
   - Right of the data subject to access information about the processing of his/her personal data (for more details, see Section 12 of Act No. 101/2000 Coll.)
   - Right to have personal data corrected, the right to request an explanation, and other rights (for more details, see Section 21 of Act No. 101/2000 Coll.).
7. In case of fundamental changes in the distribution and set-up of a camera monitoring system (this concerns changes in the purpose of processing, an increase in the number cameras, moving the cameras or cameras being directed at premises with a higher level of protection of privacy, changes in the operating regime of the camera monitoring system in terms of an

[12] *Even if camera monitoring based on the data subject's consent is to be rare in practice, consent may not be entirely left out also for the reason that Act No. 101/2000 Coll. stipulates the general rule that the controller may only process data with the data subject's consent, with an exhaustive list of the exemptions to this rule being listed in the act.*

increase in the monitoring period, prolongation of the period for storing recordings, reducing the protection of the camera system or camera recordings), the subject needs to be informed about (and consent obtained from him/her) to such fundamental changes in the processing of personal data.

8. See Annex No. 1 for consent templates:
    - In the case of template 1, information about the camera system is provided to the data subject or his/her statutory representative upon granting consent.
    - In the case of template 2, it is assumed that the data subject or his/her statutory representative has been provided with the information in a different (demonstrable way) prior to the consent being granted.
9. It is recommended that the proposed procedure to be taken by the controller or processor be drawn up in the following cases:
    - The data subject retracts consent with the processing of his/her personal data
    - There is a new data subject who does not provide consent with the processing of his/her personal data.

Consent Template 1

Consent with processing personal data via a camera monitoring system with video recording

I (*title, name, surname*) hereby grant consent to (*controllers's name, registered office, and ID No.*) to process my personal data through video recordings made using a camera monitoring system operated for the purpose of (*protection of property*,....). The (*either controller - then omit this sentence - or processor - in such case indicate name, ID No., registered office*) will be processing the personal data. The personal data will be made accessible (*in the case of extraordinary events to the criminal authorities or administrative authorities for the purpose of conducting infringement proceedings, etc.*). The camera monitoring system comprises (*number of cameras*) located (*e.g., inside the building in the main entrance, in the hallway, etc.*) at (*the registered office of the controller/processor/at the address - address of location of camera only if not the same as the controller's or processor's registered office*). The recordings will be stored for (*add number*) days and the regime of the camera system is (*continuous, based on the detection of movement, etc.*). Consent with processing is granted for *an indefinite period of time/(number) years/ (number) months.* I have been informed about my right to access my personal data in compliance with Section 12 and about my right to request an explanation or a correction of the existing state in compliance with Section 21 of Act No. 101/2000 Coll., on the protection of personal data and on amendments to certain acts, as amended.

Place, date, signature

Consent Template 2

Consent with processing personal data via a camera monitoring system with video recording

I (*title, name, surname*) hereby grant consent to (*controller's name, registered office, and ID No.*) to process personal data through video recordings made using a camera monitoring system located at (*controller's registered office - address of location of cameras if not the same as the controller's registered office*) for *an indefinite period of time/(number) years/(number) months*. Prior to granting consent, I was informed about the camera monitoring system in compliance with Section 5(4), Section 11(1), Section 12 and Section 21 of Act No. 101/2000 Coll., on protection of personal data and amendments to certain acts, as amended.

Place, date, signature

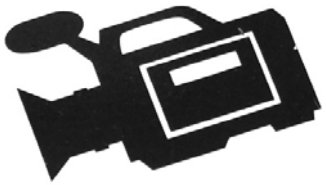
6. Marking of Premises Monitored by a Camera with a Recording Function

1. Marking of monitored premises with information signs should be carried out so that the data subject is made aware of the existence of a camera monitoring system prior to entering the monitored building or monitored premises, but in any case prior to entering the range of the camera located inside the building/on the premises.
2. The information sign has to be placed at the monitored building/premises and kept there for the entire time that the camera system is in operation.
3. The information signs have to be clearly visible, i.e., located and designed so that they cannot be overlooked.
4. The information signs have to contain at least a pictogram/picture of a camera, information about the fact that the space is being monitored using a camera monitoring and recording system, identification of the controller and a reference to the place/person where it is possible to obtain more detailed information about the camera monitoring system (e.g., telephone number, e-mail address, position of person concerned, etc.).
5. The way the information sign should look is not prescribed; it is only necessary, for obvious reasons, that the writing be clearly legible (choice of font/type and size of lettering is important).
6. The pictogram and text that the building is/premises are being monitored by a camera monitoring and recording system has to be visible/legible even from a greater distance (approx. 2-5 m).
7. Identification of the controller needs to be provided in the extent that allows verification whether the processing is registered in the public personal data processing register maintained by the Office for Personal Data Protection (accessible at www.uoou.cz). Thus, the exact name and ID No. has to be provided.
8. The reference to the place/person where it is possible to obtain detailed information should be unambiguous and the place/person easily accessible.[13]
9. In the event that visually impaired individuals are present in the building on a regular basis, it is appropriate to arrange for them to be informed in some other adequate way (audio signal, text written in special lettering, etc.).
10. In certain buildings (airports, hotels and other buildings intended for short-term accommodation, museums, etc.) frequented by visitors from outside the Czech Republic, it is appropriate to use information signs written in a number of language.

[13] *Chapter 7 describes what the content of the detailed information should be.*

Information Sign Template

Picture/pictogram of camera



Building/Premises Monitored by a Camera Monitoring and Recording System

The processing controller is (*entity's name, ID No. to be filled in*)

More detailed information about the camera system may be obtained from (*reference to a person - name and surname or title, telephone number, e-mail - or reference to a place - cash desk, reception, gatehouse, bulletin board, website*).

7. Content of Detailed Information Provided to Data Subject (Requesting Party)

The controller has the obligation to provide the data subject with information connected to his/her rights ensuing from Section 12 and Section 21 of Act No. 101/2000 Coll. For obvious reasons, detailed information cannot be included on the information sign.

1. The information should be provided in text form that can be published on the website/sent/lent for review upon request.
2. The information has to be easily accessible at least for the period that the building is/premises are accessible to authorized data subjects (e.g., during working/business hours).
3. The information has to be available for the period that personal data is being processed (from the moment that the camera monitoring system is put into operation until it the moment that it is shut down).
4. The information must be kept up-to-date.
5. Content of the information about the camera monitoring system:
    - Purposes of processing (protection of property etc.)
    - Extent of processing/category of personal data (*video recording made by camera monitoring system*)
    - Identification of controller (*name, ID No., registered office*)
    - Identification of processor, if one exists (*name, ID No., registered office*)
    - Processing location/locations (*addresses*)
    - Recipient/category of recipient/ of data made available (*e.g., criminal authorities or administrative authorities for conducting infringement proceedings etc.*)
    - Number of cameras
    - Description of location of cameras, or diagram showing location of cameras in the building or pictures of what the cameras are monitoring with a description thereof
    - Period for which recordings are stored, including manner of deletion of data following the storage period (*e.g., recorded over in a loop*)
    - Camera operation regime (e.g., *based on movement detection, continuous, outside working hours/classes*, etc.)
    - Contact information for receiving complaints (*e.g., how, when and to whom it is possible to lodge complaints; for more details see Section 21 of Act No. 101/2000 Coll.*).

8. Provision of Personal Data from a Camera Monitoring System[14]

1. The entities to which requests should be filed for the provision of a recording from the camera monitoring system are as follows:
    - Entities to which the controller is obliged to hand over recordings from the camera monitoring system based on the law, especially the criminal authorities and administrative authorities for conducting infringement proceedings.
    - Data subject or his/her statutory representative (for more details see Section 12 of Act No. 101/2000 Coll.).
    - Entities (e.g., residents, family members, employees, the mass media etc.), to which camera recordings are provided based on the consent of the data subject who is captured on the recordings.
2. Entities requesting the controller to provide the recording from the camera monitoring system should send the controller a request containing a specification the scope of the required recording, the reason for the request, and, in the case of entities to which the controller is required to provide recordings from the camera monitoring system based on the law, the deadline for providing such recording.
3. The controller may provide camera recordings to the criminal authorities or administrative authorities for conducting infringement proceedings even based on his own decision should he suspect that a crime or offense was committed and such act was recorded.
4. For the processing of the request for the provision of recordings from the camera monitoring system or provision of camera recordings based on one's own decision, the Office recommends developing procedures that will stipulate and contain the following:
    - Controller's contact person for forwarding requests for the provision of data
    - Assessment of the justification for providing the data
    - Procedure for preparing copies of recordings, including appointment of a person to arrange for such copies
    - Appointment of a person who will arrange for the copies of a camera recording to be handed over to the requesting party or the criminal authorities or administrative authorities for conducting infringement proceedings
    - Instructions for processing the document on the handover of the copies of the camera recording
        - It is possible to use the protocol on handover of the camera recordings, prepared by the criminal authorities or administrative authorities for conducting infringement proceedings without the need to draw up additional documents
        - If the document on the handover is arranged directly by the controller, the Office recommends drawing up a handover protocol or making a record in the operational journal; such record should contain the following information:
            - Date of provision of the recording

[14] *Publication of recordings by the camera monitoring system controller or provision of recordings for publication without the data subject's consent (such as placement of recordings or part thereof on a publicly accessible website, provision of recordings or part thereof for public showing or the public showing thereof, etc.), provided the recordings had not already been published in compliance with the law, e.g., by the police for the purposes of capturing a perpetrator of a crime, shall be deemed the unlawful provision of a recording.*

- Reason for providing the recording
- Identification of the party requesting the recording (in case of a request from the appropriate authorities, also the reference numbers of the pertinent proceedings or other specification of the pertinent proceedings) or the entity to which the recording is provided based on the controller's own decision
- Specification of the provided recordings (date recording made, time from - to)
- Name and surname of person handing over the recording, including his/her signature
- Name of surname of recipient of recording, including his/her signature.

5. For the purposes of providing recordings from the camera monitoring system, the Office recommends that the day of receipt of the request be the decisive date; three weeks from receipt of the request is deemed to be a reasonable period for providing a recording, or it is necessary to observe the deadline specified by the criminal authorities.
6. When providing camera recordings to data subjects, the following rules need to be observed (for details see Section 12 of Act No. 101/2000 Coll.):
    - Only those parts of the recording on which the data subject requesting the recording (the requesting party) is captured may be provided
    - No other data subject may be discernible on the recording (their image has to be distorted, the recording blurred in the respective place, etc.), unless of course the requesting party has obtained consent from such parties that he/she may obtain the recording with their data included.
7. The controller shall be entitled to reasonable compensation for the costs associated with providing the camera recording to the data subject (for more details see Section 12(3) of Act No. 101/2000 Coll.).

List of Reference Material (available on the Office for Personal Data Protection website – www.uoou.cz)

- Standpoints:
  1. Standpoint No. 1/2006 - Operation of a camera monitoring system from the perspective of the Personal Data Protection Act
  2. Standpoint No. 1/2008 - Placement of camera monitoring systems in residential buildings
  3. Standpoint No. 2/2008 - Consent to personal data processing
  4. Standpoint No. 2/2009 - Protection of employee privacy with special attention to workplace monitoring
  5. Standpoint No. 4/2009 - Activity of security agencies from the perspective of the Personal Data Protection Act
  6. Standpoint No. 5/2009 - Publication of personal data in the media
  7. Standpoint No. 9/2012 - on the possibility of municipalities to operate camera monitoring systems in public areas
  8. Standpoint No. 10/2012 - on the issue of operating webcams transmitting data to publicly accessible websites from the perspective of the Personal Data Protection Act
  9. Standpoint No. 12/2012 - on use of photographs, audio and visual recordings of natural persons
- Other documents:
  10. Commentary on the rules for operating camera monitoring systems from the perspective of the Personal Data Protection Act
  11. Commentary on the notification duty of controllers processing personal data using camera monitoring systems
  12. Camera monitoring systems installed in schools and educational institutions from the perspective of the Office for Personal Data Protection
  13. Response and recommendations of the Office for Personal Data Protection regarding the possibility to install camera monitoring systems on school premises
  14. Practical issues of operating camera monitoring systems in schools and educational institutions
- Frequently asked questions:
  15. Is it possible to broadcast regional or municipal council meetings live on television or the internet?
  16. What are the obligations of controllers processing personal data using camera monitoring systems?
  17. I am operating a camera monitoring system. Does the registration duty apply to me?
  18. Camera monitoring systems in publicly accessible buildings. Is a local governmental entity with cameras installed on its premises (halls, stairwells, building entrance) obliged to register with the Office for Personal Data Protection? There is no statutory license. Is the issue one of public interest?
- From the decision-making activities of the Office:
  19. Particulars of consent with personal data processing
  20. On camera monitoring systems at the municipal office

21. On operating a camera monitoring system at the workplace

- OPDP Information Bulletin 2/20011

Ministry of the Interior

22. Information on the standpoint of the Ministry of the Interior of the Czech Republic on personal data protection in the area of utilization of camera monitoring systems
23. Information about the standpoint of the Ministry of the Interior of the Czech Republic on publication of recordings from municipal camera operating systems

Case Law

24. Judgment of the Prague Municipal Court (1 Ca 433/2008-891 Ca 433/2008-89) - camera monitoring systems placed in a hotel
25. Judgment of the Prague Municipal Court (11 Ca 298/2008-47) - camera monitoring system in a school building
26. Judgment of the Prague Municipal Court (7 Ca 204/2005-49) - camera monitoring system in a residential building
27. Judgment of the Brno Regional Court (24 C 45/2007-121) - camera monitoring system in a residential building

Operation of Camera Monitoring Systems
Methodology for the Fulfillment of the Basic Obligations Imposed by the Personal Data Protection Act

The Office for Personal Data Protection
Pplk. Sochora 27, 170 00 Prague 7
E-mail: posta@uoou.cz
Website: www.uoou.cz

Editor: David Burian
Editing: Zbyněk Havelda
Copy editing: The Office for Personal Data Protection, Press Department
Translation: Artlingua, a.s.

The methodology was discussed on 16 October 2012 on the occasion of the round table “Camera Monitoring Systems and Their Operation from the Perspective of the Personal Data Protection Act in Theory and in Practice”, organized by ORSEC, which we thank for their cooperation.