Brussels, 17 March 2010

# THE EDPS VIDEO-SURVEILLANCE GUIDELINES

## Table of contents

## Foreword

These Guidelines provide a practical set of recommendations for European institutions and bodies on how to design and operate their video-surveillance systems. Well-designed and selectively used video-surveillance systems are powerful tools for tackling security issues. On the other hand, badly designed systems merely generate a false sense of security while also intruding into our privacy and negatively impacting other fundamental rights.

Indeed, fundamental rights and security do not have to be mutually exclusive. Using a pragmatic approach based on the twin principles of selectivity and proportionality video-surveillance systems can meet security needs while also respecting our privacy. Cameras can and should be used intelligently and should only target specifically identified security problems thus minimising gathering irrelevant footage. This not only minimises intrusions into privacy but also helps ensure a more targeted, and ultimately, more efficient, use of video-surveillance.

Within the limits provided by data protection law, each institution and body has a degree of discretion on how to design its own system. At the same time, each institution must also demonstrate that procedures are in place to ensure compliance with data protection requirements. Recommended organisational practices include adopting a set of data protection safeguards that are to be outlined in the institution's video-surveillance policy and periodic audits to verify compliance.

In some cases where the risks of infringement of fundamental rights are particularly high (for example, in case of covert surveillance or dynamic-preventive surveillance), a privacy and data protection impact assessment should also be carried out and submitted to the EDPS for prior checking. However, apart from these exceptions, there is no need to closely involve the EDPS in the decision-making on how to design a particular system.

Data protection should not be viewed as a regulatory burden, a "compliance box" to be "ticked off". Rather, it should be part of an organisational culture and sound governance structure where decisions are made by the management of each institution based on the advice of their data protection officers and consultations with all affected stakeholders.

We hope that you will find that our Guidelines are useful in your compliance efforts.

(signed)

Giovanni BUTTARELLI
Assistant European Data Protection Supervisor

# 1 Objective of the Guidelines

These guidelines ("**Guidelines**") were issued by the European Data Protection Supervisor ("**EDPS**") in the exercise of the powers conferred on him in Article 47 of Regulation 45/2001 on the protection of personal data by Community institutions and bodies[1] ("**Regulation**").

The objective of the Guidelines is to offer practical guidance to the European Union (formerly: Community) institutions and bodies ("**Institutions**")[2] operating video-surveillance equipment on how to comply with the Regulation and use video-surveillance responsibly with effective safeguards in place. They set out the principles for evaluating the need for resorting to video-surveillance and give guidance on how to conduct it in a way which minimises impact on privacy and other fundamental rights.

The Guidelines are addressed to those who decide whether to install video-surveillance systems and are responsible for their operation (the "**controllers**" in data protection terms[3]). This typically includes the security services of the Institutions but also the senior management of the Institutions ultimately responsible for decision-making. In addition, the Guidelines also aim to advise suppliers or other contractors assisting in the installation and operation (some acting as "**processors**[4]"), as well as to the Institutions' data protection officers ("**DPOs**")[5], staff representatives and the general public.

The Guidelines are not definitive statements of law. Instead, they offer recommendations and suggest best practice while acknowledging that there may be exceptions to the rule and that within the limits provided by data protection law, each Institution has a margin of discretion on how to design its own system. The Guidelines are flexible: they are designed to allow customisation. This flexibility should prevent rigid or bureaucratic interpretation of data protection concerns from hampering justified security needs or other legitimate objectives.

---

[1] Regulation 45/2001 of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L 8, 12.01.2001, p. 1.

[2] Since the entry into force of the Lisbon Treaty, the legal landscape of the European Union has changed considerably. One of the most prominent changes has been the abolition of the pillar structure, and consequently, the inclusion of the third pillar policy areas into the former first pillar area. These changes have consequences for the work of the EDPS and raise questions as to the scope of application of the existing data protection rules to European institutions and bodies. Without prejudice to any further interpretation or possible revision of Article 3(1) of the Regulation, the EDPS already offers assistance and guidance to all Institutions when appropriate and recommends them following these Guidelines.

[3] See Article 2(d) of the Regulation.

[4] See Article 2(e) of the Regulation.

[5] See Article 24 of the Regulation.

With that said, following the guidance is often the most efficient way to comply with the law. It will also enhance the effectiveness and security of the systems, and increase the trust that staff and the public will have in the organisation. In addition, the Guidelines are also more than a non-binding collection of best practice. Indeed, they contain an authoritative interpretation of the law by the EDPS. Compliance with the Guidelines will be taken into account by the EDPS in the event of the use of his enforcement powers. Thus, it may affect whether an Institution will be subject to inspection and other enforcement action, including

- warning and admonishment[6],
- order to erase data[7],
- a ban on the processing[8], or
- a reference of the matter to the Institution's "hierarchy", to the Parliament, the Council, the Commission or the European Court of Justice[9].

# 2 Scope of the Guidelines

## 2.1 Scope

The Guidelines are applicable to video-surveillance carried out by the Institutions or by another party on their behalf for any purpose where cameras capture personal data as defined in the Regulation.

The Guidelines focus on video-surveillance for typical security purposes including access control. However, the Guidelines are also applicable to:

- more complex or more specific security operations,
- video-surveillance used during internal investigations (whether or not related to security) and
- video-surveillance used for any other purpose.

## 2.2 Exclusions from scope

The Guidelines do not apply to

- video-phone calls and video-conferencing,
- simple video-entry systems without recording[10],

[6] Article 47(1)d) of the Regulation.

[7] Article 47(1)(e).

[8] Article 47(f).

[9] Article 47(1)(g) and (h).

[10] By this we mean a simple system which allows a receptionist or security guard to remotely open a closed door

- camera use for artistic or journalistic purposes (such as for film making or to record or broadcast newsworthy events)[11],
- cameras used for scientific purposes in controlled laboratory environments, provided that they only monitor processes (e.g. physical or chemical processes) rather than individuals,
- recording or broadcasting events such as conferences, seminars, meetings, or training activities for documentary, training, or similar purposes, and
- recording or broadcasting meetings of EU decision-making bodies to increase transparency (e.g. the live transmissions of the plenary sessions of the European Parliament).

These and other potential uses, while they may fall under the Regulation, and thus, may require appropriate data protection safeguards, are not discussed in these Guidelines. Therefore, their compliance needs must be assessed by the Institutions on a case by case basis.

## 2.3 Clarifications on scope

### 2.3.1. Do the Guidelines cover devices other than CCTV systems?

For purposes of these Guidelines, video-surveillance is defined as the monitoring of a specific area, event, activity, or person by means of an electronic device or system for visual monitoring. Typically the Institutions operate CCTV systems, that is, "closed circuit television systems" comprising of a set of cameras monitoring a specific protected area, with additional equipment used for transferring, viewing and/or storing and further processing the CCTV footage. However, using any other electronic device or system, fixed or mobile, also comes under the scope of the Guidelines if it is capable of capturing image data. For example, portable video-cameras, cameras taking still images, webcams, infra-red cameras and heat recognition devices.

### 2.3.2. What is personal data?

Personal data is defined by the Regulation as “any information relating to an identified or identifiable natural person”. The Regulation also specifies that “an identifiable person is one who can be identified, directly *or indirectly*, in particular by reference to an identification number or one or more factors specific to his or her physical, psychological, mental, economic, cultural or social identity.”[12] What does

---

(e.g. main door or a garage door) to let in visitors who have no access badges for automated access. The system is activated by the visitors themselves by “ringing the bell”. This exception should be construed narrowly and should not be applied to more complex systems or systems where, although no recording takes place, the visitors are in the field of coverage of security cameras without initiating contact themselves. Compare with the example in 2.3.4 below.

[11] The Guidelines, however, apply to the transfer of video-surveillance footage, which has been collected for a different purpose, to the media. See Section 10 for a general framework of transfers.

[12] See Article 2(a) of the Regulation and Opinion 4/2007 of the Article 29 Data Protection Working Party on the concept of personal data, in particular, pages 16 and 21 thereof.

this mean in practice?

Firstly, recognisable facial images always constitute personal data. This is the case even if the individuals are not known to or not identified by the operators of the system.

*Example:*

*Your Institution installs video-cameras monitoring a locked archive room during the night and on weekends with the intention to capture recognisable facial images and identify the perpetrator of any unauthorised access. The Guidelines apply even if you only recorded the images but never reviewed the recordings.*

However, there is often no need to capture recognisable facial images for the Guidelines to apply. Less clearly visible images of an individual may also constitute personal data provided that the individuals are directly or indirectly (combined with other pieces of information) identifiable. Whether an individual can be considered indirectly identifiable depends on the circumstances of the case, including the purpose of the video-surveillance and the likelihood that the Institution (or other potential recipients) will be able to make all the efforts that are necessary to identify the persons captured on camera.

*Example:*

*Cameras are installed on the rooftop of a building with limited resolution to monitor the overall situation in the surrounding area for security purposes during special events. Although the camera footage may not always yield recognisable facial images, police, investigating a serious criminal offence, may be able to indirectly identify the persons captured on the cameras using information derived from the camera footage (for example, clothing, body type, objects carried) in combination with other information detected during the investigation (for example, with the help of witnesses or using other image recordings). In such situations, the Guidelines apply.*

Further, video-footage containing objects that may be linked to an individual may also be considered as personal data, depending on the circumstances of the case.

*Example:*

*A CCTV system, which monitors vehicle number plates, is further connected to a database containing number plate registration data. It is also equipped with software capable of reading number plates and matching those with the person in whose name the vehicle is registered. This system comes under the Guidelines even if individuals are not captured on the cameras, only number plates.*

Finally, the Guidelines apply even if an Institution does not intend to capture images that are capable of identifying the persons captured on the cameras, provided that identifiable persons are, indeed, captured on the cameras.

*Example:*

*A webcam is installed to promote a tourist location. The Guidelines apply even if the intention of the operator of the camera was not to identify the persons caught on the cameras.*

### 2.3.3. Do only permanent video-surveillance systems come under the scope of the Guidelines?

No, the Guidelines apply even if the cameras are only used on an *ad hoc* basis.

*Example:*

*Upon repeated occurrence of theft, a video-camera is installed at the entrance of a previously unmonitored storage room for a limited period of time (one week) to deter theft or investigate it if it occurs despite the presence of the cameras. The video-surveillance comes under the scope of the Guidelines despite its temporary and ad hoc character.*

### 2.3.4. Do the Guidelines apply if no footage is recorded?

Yes, live video-monitoring or live video-broadcast also come under the scope of the Regulation and the Guidelines.

*Example:*

*The security cameras monitor exits and entrances to a building: the footage is not recorded but viewed by security personnel in a control room or at the building reception. The Guidelines apply.*

Indeed, privacy and security risks may be present even if no footage is recorded and the footage is only transferred live to the intended recipients via an internal network. The risks include, for example, that the images may be intercepted by hackers, or recorded and subsequently used for incompatible purposes by one of the recipients. Importantly, the intrusion into privacy and the impact on the behaviour of those subject to surveillance will often be comparable to the intrusion and impact of recordings. In general, the privacy and data protection risks tend to increase as the number of recipients increase and are especially high if the video footage is posted on the internet.

### 2.3.5. What if the surveillance is carried out by an outsourced company?

If an Institution out-sources all or part of its video-surveillance activities to a third party (a "**processor**") it remains liable for compliance with the Regulation as a "controller".

*Example:*

*The security guards monitoring live video-footage in the reception area of an Institution work for a private company to whom the Institution outsourced the task of live monitoring. In this case the Institution must ensure that the security guards carry out their activities in compliance with the provisions of the Regulation and the Guidelines.*

For more guidance on outsourcing please refer to Section 14.1 below.

# 3 Privacy by design

## 3.1 Building privacy into the design of the system

Data protection and privacy safeguards should be built into the design specifications of the technology that the Institutions use as well as into their organisational practices[13].

## 3.2 Addressing data protection issues early on

When installing or updating a video-surveillance system, an initial data protection assessment should be carried out with the assistance of the DPO well before a tender for new acquisitions is issued or any financial commitments are made. This will help prevent costly mistakes.

[13] WP Opinion 168 of 1 December 2009 on the "The Future of Privacy", joint contribution by the Article 29 Data Protection Working Party and the Working Party on Police and Justice to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data. See, in particular, Chapter 4.

*Example:*

*As the head of the security unit of your Institution, you perceive a need for an upgrade of the existing video-surveillance system, which requires the purchase and installation of additional cameras and new software. It is important to carry out at least a preliminary analysis at an early stage as it may lead not only to the adoption of specific data protection safeguards, but also to changing the tender specifications for the suppliers. It may even require decreasing the scale of the proposed investment.*

### 3.3 Impact assessment

The EDPS recommends that a privacy and data protection impact assessment should be carried out before installing and implementing video-surveillance systems whenever this adds value to the Institution's compliance efforts[14]. The purpose of the impact assessment is to determine the impact of the proposed system on individuals' privacy and other fundamental rights and to identify ways to mitigate or avoid any adverse effects.

The effort that is appropriate to invest in an impact assessment depends on the circumstances. A video-surveillance system with large inherent risks, or one raising complex or novel issues, warrants investment of much more effort than one with a comparatively limited impact on privacy and other fundamental rights, such as a conventional static CCTV system operated for typical security purposes for which the Guidelines already provide adequate safeguards.

In any event and in all cases, whether in a formal impact assessment or otherwise, the Institutions must assess and justify whether to resort to video-surveillance, how to site, select and configure their systems, and how to implement the data protection safeguards proposed in the Guidelines.

In addition, there may be cases where an Institution proposes a non-standard system. In this case the Institution should carefully assess the planned differences from the practice and recommendations set forth in the Guidelines, discuss these with their DPO and with other stakeholders, and document its assessment in writing, whether in a formal impact assessment or otherwise. The institution’s audit of the system (see Section 13) should also address the lawfulness of the customisation of the system.

Finally, due to their complexity, novelty, specificity, or inherent risks, the EDPS strongly recommends carrying out an impact assessment in the following cases:

[14] For systems which are already in operation at the date of coming into force of these Guidelines, the impact assessment should be carried out retroactively. See Section 15 for more detail on transitory provisions and how to ensure compliance for existing systems.

- video-surveillance for purposes other than security (including for investigative purposes, see Section 5.8),
- employee monitoring (Section 5.9),
- webcams (Section 5.10),
- monitoring on Member State territory and in third countries (Sections 6.5-6.6);
- special categories of data (Section 6.7);
- areas under heightened expectations of privacy (Section 6.8);
- high-tech and/or intelligent video-surveillance (Section 6.9);
- interconnected systems (Section 6.10);
- covert surveillance (Section 6.11);
- sound-recording and "talking CCTV"(Section 6.12).

The impact assessment may be carried out in-house or by an independent contractor. The assessment should be conducted at an early stage of the project. Based on the results of the impact assessment an Institution may decide

- to refrain from or modify the planned monitoring and/or
- to implement additional safeguards over and above those in these Guidelines.

The impact assessment should be adequately documented. As a matter of principle, an impact assessment report should clearly specify the risks to privacy and/or other fundamental rights that the Institution identified and the additional safeguards proposed.

*Example:*

*Your Institution considers the installation of a complex dynamic-preventive video-surveillance system. This may be permissible only subject to a comprehensive privacy and data protection impact assessment by the Institution (and subject to all other safeguards provided for in these Guidelines or recommended by the EDPS in a prior checking procedure).*

### 3.4 Using privacy-friendly technology

Whenever possible, privacy-friendly technological solutions should be used. When commissioning the system and drafting tender specifications, contractors should be invited and incentivised to offer such solutions.

*Examples:*

- Encrypting data may reduce the potential damage in case of unauthorised access to the images. See also Section 9 below.
- Masking or scrambling images to help eliminate surveillance of areas irrelevant to your surveillance target. This technique is also useful to edit out images of third persons when providing access to the images of a data subject. See also its use to protect facial images or number plate information when operating a webcam (Section 5.10).

### 3.5 Planning ahead for *ad hoc* surveillance

Finally, advance plans should also be made when an Institution contemplates using video-surveillance on an *ad hoc* basis (for example at times of hosting high-profile events or during internal investigations). In this case the necessary framework and policies for data protection should be established sufficiently before the occurrence of the video-surveillance itself.

*Examples:*

- *Your Institution regularly hosts high-profile events such as meetings of heads of States and governments, with increased security needs at such times.*
- *You foresee that from time to time there might be a need to install and use cameras during internal investigations at certain locations for limited periods of time on an ad hoc basis.*

## 4 Who should be consulted about the new system

Consultation with stakeholders and competent authorities is essential in order to identify all relevant data protection concerns. When deciding whether to use video-surveillance and establishing the necessary framework and policies for data protection, some or all of the following individuals or organisations may need to be consulted:

- the DPO of the Institution,
- employee representatives,
- other stakeholders (including, in some cases, local authorities),
- the EDPS and
- national (or regional) data protection authorities.

### 4.1 Data Protection Officer

First and foremost, the plans to install or update a video-surveillance system should be communicated to the DPO of the Institution. He or she should be consulted in all cases and should be involved in all stages of the decision-making.

*Examples:*

- *The DPO should be participating in the initial determination whether to use video-surveillance technology, as discussed in Section 3.2.*
- *The DPO should be called upon to provide expert advice on developing data-protection-friendly procedures.*
- *He or she should also be called upon to comment on the Institution's draft video-surveillance policy (including its attachments), and to correct mistakes and suggest improvements.*
- *His or her assistance should also be sought in your communications with the EDPS and national (or regional) data protection authorities.*

### 4.2 Staff and other stakeholders

The EDPS strongly recommends that staff should be consulted in all cases where staff members may be captured on cameras. Consultation is recommended even if the purpose of the processing is not to monitor or evaluate the performance of staff members. Further, consultation is mandatory where legally required by applicable law. Staff can typically be consulted via the staff committees operating in the Institutions but other means (for example, public consultations and workshops), may also be effective.

*Example:*

*Staff should be consulted even if the purpose of the processing is security and access control and the cameras are only installed at entrances and exits of the buildings and certain other strategic locations such as archive rooms.*

Consultation does not mean that management must in all cases reach an agreement with staff representatives regarding the extent of monitoring. However, the EDPS considers a genuine consultation as a particularly important safeguard to ensure that the video-surveillance installed will not be more intrusive than necessary and that adequate safeguards will be introduced to minimise any risks to privacy and other legitimate interests and fundamental rights.

If there are other stakeholders present, due to the location or specific nature of the video-surveillance, the Institution should ensure that those stakeholders or their representatives are also consulted as widely as possible. This also includes consultation with local governments, police or other bodies in the cases referred to in Sections 6.5 and 6.6.

*Example:*

*Parents should be consulted when video-surveillance involves the child care facilities operated by your Institution.*

### 4.3 Prior checking by the EDPS

In some cases the DPO of the Institution must submit a prior checking notification to the EDPS[15]. The aim of this procedure is to assist the Institution in establishing additional data protection safeguards in cases where its activities go beyond the standard operations for which the Guidelines already provide sufficient safeguards. During the prior checking procedures the Institutions' compliance with the recommendations set forth in these Guidelines may also be verified.

Currently the EDPS considers that a prior checking notification is required for the following cases:

- video-surveillance proposed for investigative purposes (Section 5.8),
- employee monitoring (Section 5.9),
- processing of special categories of data (Section 6.7),
- monitoring areas under heightened expectations of privacy (Section 6.8),
- high-tech or intelligent video-surveillance (Section 6.9),
- interconnected systems (Section 6.10),
- covert surveillance (Section 6.11),
- sound-recording and "talking CCTV" (Section 6.12).

The notification must include the impact assessment report (or other relevant documentation on the impact assessment), the video-surveillance policy and the audit report (see Section 13 below).

### 4.4 National Data Protection Authorities

The provisions of the Regulation apply[16] and the EDPS is competent to supervise all video-surveillance carried out by or on behalf of the Institutions, irrespective of whether they capture images within the buildings of the Institutions or outside those buildings. With that said, the data protection authorities of the Member State in which the Institution is located may also have an interest with respect to monitoring that takes place outside the buildings. In this case, the applicability of national data protection law, in any event, is limited by the privileges and immunity enjoyed by the Institutions pursuant to Article 291 EC Treaty and Protocol (No 36) on the privileges

[15] See Article 27 of the Regulation, which requires that "processing operations likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope, or their purposes shall be subject to prior checking by the European Data Protection Supervisor".

[16] See Articles 3(1) and 41(2) of the Regulation.

and immunities of the European Communities (1965)[17]. The EDPS will cooperate with data protection authorities in Member States, should the need arise[18].

Section 6.5 provides a set of recommendations aimed at minimising monitoring on Member State territory. These recommendations should encourage good data protection practice, but also, prevent, or minimise, the duplication of effort and the uncertainty that may arise from concurrent applicability of two data protection regimes and concurrent action of two supervisory authorities.

In addition to these substantive recommendations, as a matter of procedure, the EDPS further recommends that Institutions should always submit at least a brief letter to the national data protection authority (and/or regional or local data protection authority, if relevant) concerned during the preliminary consultation process. In the letter, the Institution should inform the authority that it operates a video-surveillance system within its buildings for security and access control and the system also captures images in the vicinity of its buildings. The letter should confirm that these practices are in compliance with the provisions of these Guidelines and the Regulation and subject to the supervisory authority of the EDPS (and will be subject to prior checking by the EDPS if applicable). A copy or link to the Guidelines should also be provided. Should the national data protection authority require further information, the Institution should cooperate in good faith. As a matter of good practice, the final EDPS prior checking opinion, when applicable, may also be sent to the competent data protection authority.

# 5 Deciding whether to use video-surveillance

The decision to use video-surveillance systems should not be taken lightly and requires a careful assessment of the potential benefits and its impact on the rights to privacy and other fundamental rights and legitimate interests of those in the area of coverage. Whenever possible, the decision should be documented in writing, and adequately supported by evidence such as statistical data on the actual number of security incidents that occurred, as well as evidence of past effectiveness of the cameras to deter, prevent, investigate, or prosecute these incidents. The existence of a written justification whether to use video-surveillance and its adequacy, should be verified and assessed during the audit (see Section 13).

This analysis, however, does not always have to be an extensive or time-consuming process. The extent of assessment will depend on the size of the proposed scheme and the level of impact it is likely to have on people's privacy and other legitimate interests or fundamental rights. In their assessment, the Institutions must address the following questions:

- What are the benefits to be gained from the use of video-surveillance and do they outweigh its detrimental effects?

[17] Official Journal C 321 E, 29/12/2006 P. 0318 - 0324. Note that some of the so-called "headquarters agreements" concluded between the Institutions and their host countries specifically state that national data protection laws shall not apply to the Institution. This is the case, for example, with the European Central Bank.

[18] See Article 28(6) of the Directive and Article 46(f) of the Regulation.

- Is the purpose of the system clearly specified, explicit and legitimate? Is there a lawful ground for the video-surveillance?
- Is the need to use video-surveillance clearly demonstrated? Is it an efficient tool to achieve its intended purpose and are there less intrusive alternatives available?

The guidance in this document will help the Institutions decide where video-surveillance may be an appropriate tool to be used. For existing systems[19], many Institutions may find that all they need to do is to be more explicit and transparent, and confirm in writing their existing good practices.

## 5.1 Purpose of the system

Before deciding to install a new system the Institution must first establish the purpose of the video-surveillance and must make sure that this purpose is legitimate[20].

**5.1.1 Be clear, specific and explicit.** Vague, ambiguous, or simply too general descriptions are not sufficient. Being specific about the purpose of the video-surveillance can help the Institutions to comply with the law, assess the success of their system, and explain to their staff and members of the public why it is needed.

**5.1.2. Communication of the purpose to the public.** The purposes of the system 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 Institution's video-surveillance policy[21].

**5.1.3. Further incompatible use and function creep[22].** The limitations on the use of the data must be clearly established especially if this is requested by staff representatives or other stakeholders.

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 ("**function creep**"). 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. A broad high level definition of purpose does not justify further use for unspecified purposes.

---

[19] See Section 15 on transitory provisions.

[20] See Regulation, Article 4(b).

[21] See Section 11 and Appendices 1 and 2 for further guidance on how to provide notice to the public.

[22] See Article 4(b) of the Regulation on incompatible use.

*Example:*

*When a video-surveillance system is installed for security purposes and was announced as such to staff, recordings should not be used to assess how well staff perform their job or whether they come to work on time. Neither should it be used as an investigative tool or evidence in internal investigations or in disciplinary procedures, unless a physical security incident or, in exceptional cases, criminal behaviour is involved.*

### 5.2 Is there a lawful ground for video-surveillance?[23]

If an Institution uses video-surveillance for typical security and access control purposes, then this can be deemed as *potentially* necessary for the management and functioning of the Institution. Therefore, the video-surveillance system will be based on a lawful ground, as required under the Regulation[24].

If this is not the case, the question arises whether there are any other possible lawful grounds for video-surveillance. Examples of available grounds for lawfulness can be situations where there is a legal obligation to carry out video-surveillance or where individuals concerned have given their unambiguous consent[25]. .

### 5.3 Is the need to use video-surveillance clearly demonstrated?

Once the purpose of a video-surveillance system is established, and there is a lawful ground for its use, one should justify that camera use is indeed *necessary* in the Institution's specific circumstances [26].

### 5.4 Is video-surveillance an efficient tool to achieve its purpose?

Systems should not be installed if they are not effective in achieving their purposes, for example, if they merely provide the illusion of greater security.

---

[23] See Article 5 of the Regulation.

[24] See Article 5(a) and recital 27 of the Regulation.

[25] See Articles 5(b) and (d).

[26] See Regulation, Article 5(a),(b), (c), (e). (In case the video-surveillance is based on consent, you need to make sure that the video-surveillance does not go beyond what is necessary to achieve the purpose for which the individuals gave their consent.)

*Example:*

*If the purpose of your system is to control access to various parts of a large building which are not physically separated by locked doors or other access control systems, a set of one hundred cameras with footage recorded and remotely viewed from a control room by two CCTV operators will not help you prevent unauthorised access, and at best, may only help you investigate a security incident after it happened.*

### 5.5 Are less intrusive alternatives available?

The Institution must also assess whether there is a less intrusive method to achieve the intended purpose, without the use of cameras. Video-surveillance should not be used if adequate alternatives are available. An alternative can be considered adequate unless it is not feasible or significantly less effective than video-surveillance or would involve disproportionate costs.

Mere availability of the technology at a relatively low cost is not sufficient to justify the use of video-technology. One should refrain from simply making the choice which appears to be the least expensive, easiest and quickest decision but which fails to take into account the impact on the data subjects' legitimate interests and the effect on their fundamental rights.

*Example:*

*You should not install a video-surveillance system to monitor the area of your info-centres offering internet access to visitors, merely for the purpose of monitoring availability of space. As an alternative, a software application can be installed tracking the number of logged on and logged off computers at each info-centre at any time.*

### 5.6 Do the benefits outweigh the detrimental effects?[27]

Finally, even if an Institution concludes that there is a clear need to use video-surveillance and there are no other less intrusive methods available, it should only use this technology if the detrimental effects of video-surveillance are outweighed by the benefits of the video-surveillance.

[27] See Article 4(1)(c) of the Regulation and Articles 8 and 52 of the Charter of Fundamental Rights of the European Union. Other relevant provisions on fundamental rights include, among others, Articles 7, 11, 12, 21 and 45 of the Charter. See also the European Convention on Human Rights, in particular, Articles 8, 10 and 11 and Protocol 4, Article 2, as well as Article 13 of the Treaty Establishing the European Communities.

It is obvious that video-surveillance should not be used where this would be clearly excessive compared to the benefits derived from it.

*Example:*

*You should not install a camera in the communal kitchen and lunch room, to help prevent or detect those who "help themselves" to items left in the fridge or cupboards by other staff members even if (i) notice is provided, (ii) this is a recurring problem and (iii) other means to remedy the problem failed.*

However, in many cases, the analysis becomes more complex and the legitimate interests and fundamental rights of the people monitored may need to be balanced very carefully with the benefits that may be achieved by the surveillance.

### 5.7 Security purposes

If the video-surveillance is carried out for security purposes, the Institutions should carefully evaluate risks, and not merely state that the purpose is to "observe any anomalies inside the security perimeter", or "to deal with security incidents". Indeed, the Institutions should not only have a general idea of what they wish to use their system for, but should also detail the types of security incidents that are expected to occur in the area under surveillance and that they wish to deter, prevent, investigate or prosecute using the cameras.

Generally, when defining the purpose, the Institutions should make clear that the video-surveillance system helps control access to the buildings and helps ensure the security of the buildings, the safety of staff and visitors, as well as property and information located or stored on the premises.

They should also specify whether the video-surveillance system is designed to prevent, deter, investigate and/or prosecute security incidents (by securing evidence)[28].

They should not simply identify any security risks that may potentially exist but must also justify, in a realistic and verifiable manner, the existence and extent of those risks (specific dangers, crime rates, etc). Mere "perception" of a risk, speculation or anecdotal evidence is not sufficient to justify the necessity of video-surveillance. This risk analysis should be documented in writing and should identify and assess any existing risks. Indeed, the Institutions need to demonstrate the type of security risks in the area under surveillance by showing what security incidents occurred there in the past or are likely to occur there in the future.

[28] Video-surveillance may, at times, help prevent security incidents either by deterring potential perpetrators or by allowing a quick response to emergency situations. In practice, however, rather than preventing security incidents, video-surveillance often merely serves to investigate them after the fact, and secure evidence, should such incidents occur. You must be very clear on what you are trying to accomplish.

*Examples:*

*You should specifically and individually consider and evaluate the potential use of video-surveillance for each of the following different types of security incidents, where applicable:*

- *unauthorised physical access to specific secure premises and protected rooms (e.g. rooms containing critical IT infrastructure or sensitive operational information)*
- *theft of personal belongings of staff members (e.g. laptops, mobile phones, handbags, jackets left unattended in individual offices or in meeting rooms)*
- *bicycle thefts or car break-ins in your parking lot*
- *security threats during international summits and other special events*
- *equipment malfunctioning at nuclear research facilities*
- *physical attacks against your buildings (throwing of stones, break-in, vandalism, etc) during protests and demonstrations*
- *physical assault of your security personnel at the main entrance during protests and demonstrations*

*This list is only illustrative.*

Once risks are identified, there is also a need to ask a more complete set of questions to establish not only the existence of specific threats but also that video-surveillance is the right tool to be used to counter these threats. As explained in Sections 5.4 - 5.6, it must be established that video-surveillance is an efficient tool to achieve its purpose, that there are no other less intrusive alternatives available, and that the benefits outweigh any detrimental effects. Importantly, before opting for video-surveillance, all other less intrusive alternatives should be carefully considered. These may include, for example, controls by security personnel, upgrading alarm systems, access control systems, armouring and reinforcing gates, doors and windows and better lighting. Only when such solutions are demonstrated to be insufficient, should video-surveillance be used.

### 5.8 Investigative purposes

Where a system is set up for typical security purposes, the video-recordings can be used to investigate any physical security incident that occurs, for example, unauthorised access to the premises or to protected rooms, theft, vandalism, fire, or physical assault on a person. Indeed, in addition to deterrence and prevention, the video-surveillance system almost always also serves the purposes of investigating the facts after the occurrence of a security incident, and obtaining evidence to prosecute the perpetrator. However, in principle, video-surveillance systems should not be installed or designed for the purposes of internal investigations beyond physical security incidents such as those noted above.

With that said, it cannot be excluded that in exceptional circumstances, video-

surveillance technology might nevertheless also be used for investigative purposes, even when it is not directly triggered by a physical security incident. To decide whether these uses are permissible, and whether they require additional safeguards not provided for in these Guidelines, a case-by-case analysis is necessary. Therefore, your policy on any such proposed video-surveillance is subject to impact assessment by your Institution and prior checking by the EDPS.

*Examples:*

- *Cameras are installed at a locked archive room for security and access control purposes and the footage is monitored live by the security guard in the reception area. The cameras also record the footage. At 4 am, the alarm system rings signalling unauthorised access. Subsequent investigation of the security incident using the CCTV footage shows that the day before repair work was carried out on the air conditioning system of the archive room and a window was opened and inadvertently left open. This investigation is appropriate and within the scope of a typical security purpose.*

- *You wish to use the CCTV system in a targeted way to investigate the daily activities of Mr. X, a desk officer at your Institution who is suspected of having committed procurement fraud, benefit fraud, having harassed a work colleague, or having been drunk while at work. This would go beyond the security and access control purpose and require both an impact assessment and prior checking.*

### 5.9 Employee monitoring

Overly intrusive monitoring measures can cause employees unnecessary stress and can also erode trust within the organisation. The use of video-surveillance to monitor how staff members carry out their work should therefore be avoided, apart from exceptional cases where an Institution demonstrates that it has an overriding interest in carrying out the monitoring.

Therefore, any such proposed video-surveillance is subject to an impact assessment by the Institution. The Institution must also submit its plans to the EDPS for prior checking. Where the Institution proposes to use video-surveillance technology to monitor the work of staff, the EDPS will pay special attention to the views and concerns expressed by the Institution's staff representatives and whether such views were taken into account.

Goals such as managing workplace productivity, ensuring quality control, enforcing the Institutions' policies, or providing evidence for dispute resolution, alone, generally do not justify video-surveillance of employees in the context of the work of the Institutions.

*Example:*

*You should not use your existing video-surveillance system to monitor the efficiency of the outsourced cleaning staff while they carry out their work during the early morning hours even if adequate notice were to be given to them in this regard, and repeated complaints arose regarding their quality of work.*

Further, practices whereby an employee is under constant surveillance (continuously in the field of vision of video-surveillance cameras) should be avoided.

*Example:*

*You should not use video-surveillance cameras to continuously monitor the cashier and the cash register in the canteen during opening hours even if adequate notice were to be given to the cashier in this regard.*

As for monitoring triggered by security or health and safety concerns or similar compelling interests in exceptional circumstances, the EDPS will evaluate any such justifications on a case-by-case basis.

### 5.10 Webcams

For purposes of these Guidelines, a webcam is a digital video capture device connected to the internet and supplying a view for anyone who visits its web page. Devices connected to the Institution's intranet, or to websites which are not available to the general public, but only to a specific audience (such as participants to an event) are also considered as webcams for the purposes of these Guidelines.

Webcams provide opportunities, for example, enhancing education, communication and recreation. However, webcams may give rise to specific data protection risks. Many of these risks are connected to the lack of control by the operator of the webcam on who will view and use the images and for what purposes. Webcams capture and transmit digital images that are instantaneously broadcast to a multitude of recipients. These images can be easily recorded, copied and further distributed by any one of these recipients. The digital records holding continuous, detailed information may then be conveniently stored, searched and indexed for infinite replay and analysis. Videos recorded today might still be available online for many years to come - containing people's "digital footprint". Ultimately, there is an increased risk that the images will be misused.

When compared with the benefits of webcam use - which is often only little more than pure "entertainment" - these risks are often not justified. There are also often other readily available and less intrusive alternatives to achieve the same purposes. For these reasons, installation of webcams must always be very carefully considered. Webcams should normally not be installed for frivolous purposes, or to promote recreational facilities offered by the Institution or a tourist location (e.g. visitors centre

fitness centre, cafeteria, visitors gallery in a meeting room).

In exceptional cases the use of webcams may nevertheless be permissible based on the informed and individual consent of each user of the facility. Special attention should be paid to the views and concerns expressed by staff representatives and/or other stakeholders.

*Example:*

*You wish to promote a new visitors' centre by placing a video-camera on the premises with live broadcast to your Institution's internet website. The EDPS discourages this practice on grounds that many users may find the presence of the cameras intrusive. If a significant proportion of the users nevertheless show interest in being filmed, you may resort to this practice but only based on the clear and informed consent of each individual user. The users of the facility should have a genuine choice whether to use the part of the area covered by the cameras or to remain out of shot while still enjoying the facilities offered under equal terms.*

*In practice, this requires that (i) there should be only a (small) part of the facility promoted which is covered by cameras, (ii) other users in other parts of the facility can use the facilities under the same conditions as available in the promoted area, and (iii) there is a clearly visible and very conspicuous notice displayed in the area. In this case using the specific sign-posted part of the facility may constitute implied consent.*

Another important factor to consider when designing a system is the extent to which individuals are identifiable: A bird's eye view of a building with low-resolution is much less intrusive than images where the faces of the individuals can be recognised. Adverse effects on privacy can sometimes also be reduced by using software to mask any detail in the images that may help identify an individual (e.g. faces or number plates). While none of these safeguards can, on their own, legitimize webcam use, they should be considered when you assess whether to use webcams.

# 6 Selecting, siting and configuring the video-surveillance system

This Section provides guidance on how to select, site and configure a system. The guiding principle in connection with all items addressed in this Section (and indeed in the rest of these Guidelines) should be to minimise any negative impact on the privacy and other fundamental rights and legitimate interests of those under surveillance[29]. The adequacy of each choice made should be verified and assessed during the audit (see Section 13).

## 6.1 Camera locations and viewing angles

Camera locations should be chosen to minimise viewing areas that are not relevant

[29] See Article 4(1)(c) of the Regulation.

for the intended purposes.

*Examples:*

- *When a camera is installed on a rooftop to monitor an emergency fire exit, care should be taken to ensure that the camera is not positioned so as to also incidentally record the terrace of a neighbouring private building.*
- *Similarly, when a camera is installed to monitor the entrance to a specifically protected room within a building, care should be taken to ensure that the camera is not positioned so as to also incidentally record the entrance to the neighbouring private office.*

As a rule, where a video-surveillance system is installed to protect the assets (property or information) of the Institution, or the safety of staff and visitors, the Institution should restrict monitoring to

- carefully selected areas containing sensitive information, high-value items or other assets requiring heightened protection for a specific reason,
- entry and exit points to the buildings (including emergency exits and fire exits and walls or fences surrounding the building or property), and
- entry and exit points within the building connecting different areas which are subject to different access rights and separated by locked doors or another access control mechanism.

*Examples:*

- *You may place cameras at the entrance to a locked archive room where you store your Institutions' important documents and which is only occasionally entered by authorised personnel to file or to retrieve documents.*
- *You rent out the top floor of your building to another Institution. The floor is secured with a door which is kept locked at all times and can only be opened with the badges of the personnel working on the top floor. You may place a camera at the elevator area of that floor, to capture anyone exiting or entering that floor from other areas of the building.*

It cannot be excluded that security requirements may warrant more extensive monitoring within some buildings. Should this be the case, such plans should specifically be discussed in the video-surveillance policy, and the Institution should justify the need for and proportionality of such additional monitoring (in an impact assessment or otherwise).

### 6.2 Number of cameras

The number of cameras to be installed will depend on the size of the buildings and the security needs, which, in turn, are contingent upon a variety of factors. The same number and type of cameras may be appropriate for one Institution and may be

grossly disproportionate for another. However, all other things being equal, the number of cameras is a good indicator of the complexity and size of a surveillance system and may suggest increased risks to privacy and other fundamental rights. As the number of cameras increases, there is also an increased likelihood that they will not be used efficiently, and information overload occurs. Therefore, the EDPS recommends limiting the number of cameras to what is strictly necessary to achieve the purposes of the system. The number of cameras must be included in the video-surveillance policy.

### 6.3 Times of monitoring

The time when the cameras are set to record should be chosen to minimise monitoring at times that are not relevant for the intended purposes. If the purpose of video-surveillance is security, whenever possible, the system should be set to record only during times when there is a higher likelihood that the purported security problems occur.

*Example:*

*Theft repeatedly occurs during the night and on weekends from a locked storage area off a busy hallway. You may install a camera near the entrance of the storage area to detect who committed the theft or to prevent it from happening (provided that appropriate notice is given). The cameras should be set to function only outside office hours.*

### 6.4 Resolution and image quality

Adequate resolution and image quality should be chosen. Different purposes will require different image qualities. For example, when identification of the individuals is crucial, the resolution of the cameras, compression settings in a digital system, the location, the lighting and other factors should all be taken into account and chosen or modified so that the resulting image quality would be sufficient to provide recognisable facial images. On the other hand, when identification is not necessary, the camera resolution and other modifiable factors should be chosen to ensure that no recognisable facial images are captured.

*Example:*

*In some situations identifying individuals is not necessary and it is sufficient that the quality of images allows detection of movement of people or flow of traffic.*

### 6.5 Monitoring on Member State territory

In case of demonstrated security needs, an Institution may monitor the areas immediately adjacent to its buildings on the territory of Member States. However, it must be ensured that such monitoring is kept to the absolute minimum that is necessary to meet the Institution's security needs. This may include entry and exit

points, including emergency exits and fire exits, as well as walls or fences surrounding the building or property.

*Example:*

*Cameras are located at the entrance of a building filming both those exiting and entering and capturing incidentally, a few square metres of the surrounding public space (providing mostly images of passers-by in a busy street). This practice is permissible. However, monitoring the windows of an apartment building opposite should be avoided. The location or direction of the cameras should be modified, the images should be masked or scrambled, or other similar measures should be taken.*

In all cases where monitoring goes beyond monitoring entry and exit points, an impact assessment should be carried out. Such additional monitoring may only be carried out in case of demonstrated security needs and subject to additional safeguards. These may include, among others, the following:

- limitation of monitoring adjacent *private* space (e.g. via masking or scrambling images),
- whenever possible, short retention periods not exceeding 48 hours (or live monitoring only),
- limitation of the zooming capabilities of the cameras, or resolution of the cameras covering the surrounding public space,
- whenever possible, limitation of monitoring to times when there are increased security needs (e.g. international summits or other special events), and
- adequate training of the operators of the video-surveillance system to ensure that the privacy of passers-by or others caught on the cameras is not disproportionately intruded upon.

The opinion of the national (or regional) data protection authorities and other competent authorities and stakeholders should also be considered.

In any case, it is important to bear in mind that the purpose of video-surveillance, as a rule, cannot be general crime prevention or maintaining law and order on Member State territory. These are the prerogatives of certain public authorities or organisations in Member States, subject to appropriate safeguards under national law. For example, local governments and/or local police may be the only ones authorised to operate such schemes. Therefore, in general, no Institution may legitimately design and install video-surveillance systems for such purposes.

However, this does not mean that the Institution cannot use its video-surveillance system for such purposes if this is carried out in cooperation with local police (and/or local government, if applicable) and otherwise in compliance with applicable national law. In this case, the EDPS recommends that an agreement to this effect be concluded in writing. Any such proposed video-surveillance should be subject to an impact assessment by the Institution.

*Example:*

*In a (hypothetical) country where your building is located video-surveillance of public space such as city parks and streets can only be carried out by the local police and is also subject to the prior approval of the local government. You receive repeated complaints that EU staff members are getting mugged while returning home late in the evening across the small park just outside your building. You should not, at your own initiative, set up cameras overlooking the park to deter the muggings. However, if local law permits, you may cooperate with local police, and subject also to the prior approval of the local government, you may install and operate a set of cameras, for example, to monitor the main walkway through the park between dusk and dawn. You should also check with the national data protection authority whether you need to comply with any additional data protection safeguards.*

Where a prior checking notification is required, the Commission should submit a single prior checking notification to the EDPS on behalf of all Commission Representations in Member States.

### 6.6 Monitoring in third countries

The provisions set forth in Section 6.5 should also apply, *mutatis mutandis*, for monitoring activities outside the territory of the European Union. As security risks and data protection rules differ very markedly outside the European Union, the EDPS urges the Commission Delegations in third countries to carry out their own independent assessment of their security needs and design their video-surveillance systems accordingly. They should also cooperate with the local authorities, to the extent this is feasible and as long as such cooperation does not jeopardize their security.

Where a prior checking notification is required**,** the Commission should submit a single prior checking notification to the EDPS on behalf of all EU Delegations in third countries.

### 6.7 Special categories of data

Video-surveillance systems should not aim at capturing (e.g. by zooming in or discriminately targeting) or otherwise processing (e.g. indexing, profiling) images which reveal so-called "special categories of data": racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and data concerning health or sex life[30].

Areas should also not be monitored where there is an increased likelihood that images revealing special categories of data will be captured on the cameras even if

[30] See Article 10 of the Regulation.

the intention is not to collect such special categories of data[31].

*Examples:*

*You should not film demonstrators or waiting rooms at the Medical Service, or install a video-surveillance system which allows the incidental recording of the waiting rooms or areas where demonstrators are protesting. You should also not place a camera at the entrance of a trade union's office or monitor the area adjacent to a religious establishment outside your building.*

An impact assessment must be carried out in case an Institution wishes to derogate from these rules. Monitoring may only be carried out subject to additional safeguards.

In case of surveillance in order to provide security during demonstrations, these additional safeguards may include, among others, the following:

- the surveillance of any peaceful protests could only be carried out in case of demonstrated security needs,
- cameras should not focus on the faces of individuals and should not seek to identify individuals unless there is an imminent threat to public safety or violent criminal behaviour (e.g. vandalism or assault),
- in the absence of the detection of a security incident, you delete the recordings of each peaceful protest within 2 hours of the end of the protest (or consider live monitoring only),
- the images will not be used for data-mining, and
- adequate training is provided to the operators of the video-surveillance system to ensure that the privacy and other fundamental rights of the participants caught on the cameras, including, importantly, their rights to freedom of assembly, are not disproportionately intruded upon.

All monitoring processing special categories of data is subject to prior checking by the EDPS.

### 6.8 Areas under heightened expectations of privacy

Areas under heightened expectations of privacy should not be monitored. These include, typically, individual offices (including offices shared by two or more people and large, open-plan offices with cubicles), leisure areas (canteens, cafeterias, bars, kitchenettes, lunchrooms, lounge areas, waiting rooms, etc), toilet facilities, shower rooms and changing rooms.

An impact assessment must be carried out in case the Institution wishes to derogate from these rules. A prior checking by the EDPS will also be required.

[31] In ordinary circumstances (e.g. when an Institution monitors entry and exit into its buildings), the mere fact that a person's facial or body image or the clothes or accessories he or she is wearing may reveal his or her race, ethnic origin, and perhaps his health condition does not, in itself, entail that the video-surveillance activity involves processing of special categories of data.

### 6.9 High-tech and/or intelligent video-surveillance

Introduction of "high-tech video-surveillance tools" or "intelligent video-surveillance systems" are permissible only subject to an impact assessment. They are also subject to prior checking. The EDPS will assess, case by case, the permissibility of the technique used and may impose, as necessary, specific data protection safeguards.

Tools falling under this category include, among others:

- linkage of the video-surveillance system with biometric data (e.g. fingerprints for access control) or with any other database, whether biometric or not (e.g. a database of photos of suspected individuals for facial recognition, or car registration data for automatic number plate recognition),
- indexing the data in the images to allow automated searches and alerts (e.g. for tracking individuals),
- facial or other image recognition or gait recognition systems,
- any type of dynamic-preventive surveillance (e.g. using automatic behaviour analysis software applications to create automated alerts based on pre-defined suspicious behaviour, movement, clothing, body language),
- a network of cameras installed, complete with a tracking software application that can track moving objects or people throughout the whole area,
- audio-based alert systems (those triggered by changes in noise patterns such as sudden shouting),
- infra-red or near-infrared cameras, thermal imaging devices and other special-use cameras that can capture images in the dark or under low-light conditions, see through walls and search under clothing (e.g. body-scanner), and
- special purpose cameras with enhanced optical and digital zooming capabilities.

Note that the following features in and of themselves do not require an impact assessment or prior checking:

- motion detection to limit video signals to events worthy of observation and recording,
- configuration of a motion detection system so as to send alarms to security staff when it identifies that someone accesses a restricted area (e.g. a locked IT room outside office hours),
- customary panning, tilting and limited optical and digital zooming capabilities.

In case of doubt whether prior checking is necessary, please consult us.

### 6.10 Interconnection of video-surveillance systems

Interconnection of an Institution’s video-surveillance system with the video-surveillance system of another Institution or of any other third parties is subject to an impact assessment. An impact assessment is also required if a single Institution operates several separate systems (for example, systems in different cities or systems at the same location but used for different purposes) and wishes to

interconnect them. A prior checking notification is also required.

### 6.11 Covert surveillance

For purposes of these Guidelines covert video-surveillance means surveillance using cameras that are

- either intentionally hidden from view, or
- are otherwise installed without appropriate notice to the public, and therefore,
- it is reasonable to assume that the individuals monitored are unaware of their existence.

If cameras are installed in areas with heightened expectations of privacy (see Section 6.8) without fulfilment of both of the following conditions simultaneously, the video-surveillance will be considered covert even if there is a general notice at the entrance of the building announcing that the building is under video-surveillance:

- there is a specific and clearly visible notice immediately on the spot (e.g. on the door of an individual office) and
- there are further specific explanations regarding the possibility of surveillance in these areas (e.g. individual offices) in a publicly available video-surveillance policy in compliance with the recommendations set forth in Section 11.

.
The use of covert surveillance is highly intrusive due to its secretive nature. Further, it has little or no preventive effect and is often merely proposed as a form of entrapment to secure evidence. Therefore, its use should be avoided.

Proposed exceptions must be accompanied by a compelling justification, an impact assessment and must undergo prior checking by the EDPS who may impose, as necessary, specific data protection safeguards.

In principle, the EDPS is unlikely to issue a positive prior checking Opinion unless all the following conditions will be satisfied:

- covert surveillance is proposed to investigate a sufficiently serious criminal offence in a formal, legally required or authorised, investigation by Member State police, other competent law enforcement agents or by competent EU investigatory bodies;
- the use of covert surveillance is in accordance with the law and has been formally authorised by (i) a judge or other official having the powers to do so according to the laws of the Member State which requested the use of covert surveillance within the Institution, or by (ii) the competent senior decision-making body of the Institution according to the written and publicly accessible policy of the Institution relevant to the use of covert surveillance (e.g. a high level executive board);
- a register is kept of all such authorizations and instances of use of covert surveillance - this register must be available for review by the DPO and the EDPS upon request;
- the cameras are installed for a strictly limited period of time and at strictly

limited locations; and further provided that

- there are no other alternatives to the use of covert surveillance to successfully investigate the case and
- the benefits derived would outweigh the violation of privacy of the individuals observed.

### 6.12 Sound recording and "talking CCTV" [32]

Due to their intrusiveness, in principle, the use of sound recording and "talking CCTV" are also prohibited, with the exception of using them as a back-up system for access control outside office hours (as a video-phone to contact the remotely located security personnel to gain access).

When the system is used as a back-up system for access control, clear notice should be provided and the cameras should only broadcast or record sound when (i) activated by the person himself or herself who was attempting to gain access, or (ii) after a specific number of failed attempts to gain access.

Additional proposed exceptions must be accompanied by a compelling justification, an impact assessment and must undergo prior checking.

## 7 How long should the recordings be kept

### 7.1 Retention period

**7.1.1 General principles**. Recordings must not be retained longer than necessary for the specific purposes for which they were made[33]. It must also be considered whether recording is necessary in the first place and whether live monitoring without recording would be sufficient.

If an Institution opts for recording, it must specify the period of time for which the recordings will be retained. After the lapse of this period the recordings must be erased. If possible, the process of erasure should be automated, for example by automatically and periodically overwriting the media on a first-in, first-out basis. Once the media is no longer useable (after many cycles of use) it must be safely disposed of in such a manner that the remaining data on it would be permanently and irreversibly deleted (e.g. via shredding or other equivalent means).

If the purpose of the video-surveillance is security and access control, and a security incident occurs and it is determined that the recordings are necessary to further investigate the incident or use the recordings as evidence, the relevant footage may be retained beyond the normal retention periods for as long as it is necessary for

---

[32] For purposes of these Guidelines "talking CCTV" means any video-surveillance configuration using loudspeakers in the area under surveillance whereby the operators of the system can "talk" to the members of the public who are under surveillance (e.g. "gentleman in brown leather jacket, please pick up the rubbish you left behind you").

[33] Regulation, Article 4(1)(e).

these purposes. Thereafter, however, they must be also erased.

*Example:*

*An agency is equipped with a video-surveillance system for security and access control. The agency must specify a period of time, for example, 3 calendar days, after which the recordings will be automatically overwritten.*

*If a security incident is detected during those 3 days while the recordings are available, for example, if a fire broke out in the parking lot of the building, the relevant footage may be kept while the incident is investigated.*

**7.1.2 Retention period for typical security purposes: one week.** When cameras are installed for purposes of security and access control, one week should in most cases be more than sufficient for security personnel to make an informed decision whether to retain any footage for longer in order to further investigate a security incident or use it as evidence. Indeed, these decisions can usually be made in a matter of hours. Therefore, Institutions should establish a retention period not exceeding seven calendar days[34]. In most cases a shorter period should suffice.

**7.1.3 Member State or third country territory: 48 hours.** In case the surveillance covers any area outside the buildings on Member State (or third-country) territory (typically those near entrance and exit areas) and it is not possible to avoid that passers-by or passing cars are caught on the cameras, the EDPS recommends reducing the retention period to 48 hours or otherwise accommodate local concerns whenever possible.

[34] See Opinion 4/2004 of the Article 29 Data Protection Working Party on the Processing of Personal Data by means of Video-Surveillance, part 7(E), page 20.

*Example:*

*Agency A and B are each equipped with a video-surveillance system for security and access control.*

*Agency A is located in a remote rural area with little or no pedestrian or car traffic in the vicinity. Its premises are surrounded by a fence overlooking open fields. Agency A may retain its recordings for longer than 48 hours (but not exceeding seven calendar days). For example, it may wish to adopt the same 3 calendar days retention period for monitoring the areas within its property and the adjacent areas outside its property.*

*Agency B is located in the heart of a busy downtown area with a train station nearby and heavy pedestrian traffic on the pavement of the streets outside its buildings. Agency B should ensure that its retention period outside its buildings is limited to 48 hours at most. It should also consider whether a shorter retention period or live monitoring would not be sufficient.*

**7.1.4 Shorter retention periods.** The EDPS may recommend shorter retention periods or live monitoring only when this is necessary to minimise the intrusion into the privacy and other fundamental rights and legitimate interests of those within the range of the cameras.

*Example:*

*Political protests are often held in front of your buildings. You submit your prior checking on grounds that special categories of data may be processed (see Section 6.7). Considering the circumstances of the case, the EDPS may recommend that, in the absence of the detection of a security incident, you delete the recordings of each peaceful protest within 2 hours of the end of the protest at the latest (or consider live monitoring only).*

### 7.2 Register of recordings retained beyond the retention period

A register - whenever possible, in an electronic form - should be held to keep track of any recording that is retained beyond the normal retention period, indicating

- the date and time of the footage and camera location,
- a short description of the security incident,
- the reason why the footage needs to be retained and
- the expected date of the review of the necessity to retain the footage any longer.

*Example of an entry to the registry:*

- *Date and time of the footage: October 1 2009, 10 am-noon*
- *Camera location: Camera nr. 5 (located near the elevator entrance in the parking lot)*
- *Short description of the security incident: A fire broke out in the rubbish bin next to the elevator entrance in the parking lot. No personal injury or damage.*
- *Reason why the footage needs to be retained: Incident needs to be further investigated by the security unit using video-surveillance footage to find out what caused the fire so lessons can be learnt and eventual protective measures could be taken.*
- *Expected date of review whether to continue to keep the footage: 15 October 2009.*

# 8 Who should have access to the images

## 8.1 A small number of clearly identified individuals on a need-to-know basis

Access rights must be limited to a small number of clearly identified individuals on a strictly need-to-know basis. It must also be ensured that authorised users can access only those personal data to which their access rights refer[35]. Access control policies should be defined following the principle of “least privilege”: access right to users should be granted to only those resources which are strictly necessary to carry out their tasks.

Only the "controller", the system administrator, or other staff member/s specifically appointed by the controller for this purpose should be able to grant, alter or annul access rights of any persons. Any provision, alteration or annulment of access rights must be made in accordance with criteria established in the Institution's video-surveillance policy.

Those having access rights must at all times be clearly identifiable individuals.

*Example:*

*No generic or common usernames and passwords should be allocated to an outsourced security company which employs several people to work for your Institution.*

The video-surveillance policy must clearly specify and document who has access to the video-surveillance footage and/or the technical architecture of the video-surveillance system, for what purpose and what those access rights consist of. In

[35] See, in this latter respect, Regulation, Article 22.2(e)

particular, one must specify who has the right to

- view the footage real-time,
- operate the pan-tilt-and-zoom ("**PTZ**") cameras,
- view the recorded footage, or
- copy,
- download,
- delete, or
- alter any footage.

Any distinction between the rights of different categories of persons must be clearly specified.

For example, those

- monitoring the images live,
- responsible for the technical maintenance of the system, or
- investigating security incidents

have different tasks and should therefore have different access rights to the system.

In-house personnel and outside contractors will also have different tasks and should therefore also have different access rights.

Access rights should be technically built into the system. For example, the user profile of one individual may allow copying recorded footage, while the profile of another only allows viewing rights.

In addition, the access policy must also clearly describe the conditions under which access rights may be exercised. For example, in which cases a person whose profile allows copying or deletion is actually authorised to copy or delete any footage.

In case the video-surveillance is carried out for purposes of security and access control, no access rights should be given to anyone other than in-house and outsourced security personnel and those responsible for the technical maintenance of the system.

*Example:*

*Outsourced security guards working in your control room may technically be allowed to view footage real-time, operate the PTZ cameras (e.g. zoom on an object), or view recorded footage on-line, but should not be given technical access to features such as copying, downloading, deleting, or altering any footage.*

*In addition, while the guards are expected to monitor the footage real time and operate the PTZ cameras as necessary to perform their monitoring tasks, they should be instructed not to use the PTZ cameras to zoom in on a target, for example, a group of people peacefully demonstrating in front of the building, or two staff members passing by, if this is not necessary to ensure the security and access control purpose for which the monitoring is carried out.*

### 8.2 Data protection training

All personnel with access rights, including outsourced personnel carrying out the day-to-day CCTV operations or the maintenance of the system, should be given data protection training and should be familiar with the provisions of these Guidelines insomuch as these are relevant to their tasks. The training should pay special attention to the need to prevent the disclosure of video-surveillance footage to anyone other than authorised individuals.

Training should be held when a new system is installed, when significant modifications are made to the system, when a new person takes up his/her duties, as well as periodically afterwards at regular intervals. For existing systems, initial training should be held during the transitory period, before 1 January 2011.

### 8.3 Confidentiality

All personnel with access rights, including outsourced personnel carrying out the day-to-day CCTV operations or the maintenance of the system, as well as the outsourced companies themselves, should sign confidentiality undertakings to ensure that they will not transfer, show, or otherwise disclose the content of any video-surveillance footage to anyone except authorised recipients.

## 9 What security measures to take to protect the data[36]

First and foremost, an internal analysis of the security risks must be carried out to determine what security measures are necessary to protect the video-surveillance system, including the personal data it processes.

In all cases, measures must be taken to ensure security with respect to

- transmission,

[36] See Article 22 of the Regulation.

- storage (such as in computer databases),and
- access (such as access to computer systems and premises).

Transmission must be routed through secure communication channels and protected against interception. Protection against interception is especially important if a wireless transmission system is used or if any footage is transferred via the internet. In these cases the data must be encrypted while in transit or equivalent protection must be provided.

Encryption or other technical means ensuring equivalent protection must also be considered in other cases, while in transit and while in storage, if the internal analysis of the security risks justifies it. This may be the case, for example, if the footage is particularly sensitive.

All premises where the video-surveillance footage is stored and also where it is viewed must be secured. Physical access to the control room and the room storing the video-surveillance footage must be protected. No third parties (e.g. cleaning or maintenance personnel) should have unsupervised access to these premises.

The location of monitors must be chosen so that unauthorised personnel cannot view them. If they must be near the reception area, the monitors must be positioned so that only the security personnel can view them.

A reliable digital logging system must be in place to ensure that an audit can determine at any time who accessed the system, where and when. The logging system must be able to identify who viewed, deleted, copied or altered any video-surveillance footage. In this respect, and elsewhere, particular attention must be paid to the key functions and powers of the system administrators, and the need to balance these with adequate monitoring and safeguards.

A process must also be in place to appropriately respond to any inadvertent disclosure of personal information. This should include, whenever possible, notification of the breach to those whose data are inadvertently disclosed as well as to the Institution's DPO.

The security analysis as well as the measures taken to protect the video-surveillance footage must be adequately documented and must be made available for review to the EDPS upon request.

Finally, the Institution must act with due diligence in its choice and supervision of outsourced staff.

# 10 Transfers and disclosures

## 10.1 General framework

There are three main rules in the Regulation governing transfers, depending on whether the recordings are transferred (i) to a recipient within the Institution or in another Institution, (ii) to others within the European Union, or (iii) outside the

European Union[37].

For the first case, the Regulation provides that the recordings can be transferred to others within the Institution or in another Institution if this is necessary for the legitimate performance of tasks covered by the competence of the recipient. (For details and examples, please see Section 10.3.)

For the second case (transfers outside the Institutions but within the European Union), these are possible if this is necessary for the performance of a task carried out in the public interest or subject to the exercise of public authority, or if the recipient otherwise establishes that the transfer is necessary and there is no reason to assume that the legitimate interests of those whose images are transferred might be prejudiced. (For details and examples, please see Section 10.4.)

Thirdly, transfers outside the European Union can be made (i) if done solely to allow the Institution's tasks to be carried out[38] and (ii) only subject to additional requirements, mainly to ensure that the data will be adequately protected abroad. (For details and examples, please see Section 10.4.)

However, when assessing the lawfulness of a transfer, many other provisions of the Regulation must also be taken into account, which set additional conditions before a transfer can be made. Importantly, in most cases no transfer can be made for purposes that are incompatible with the initially specified purpose of the video-surveillance system.

*Example:*

*If the video-surveillance system is installed for security purposes and was announced as such, the recordings cannot then be transferred to a staff member's supervisor who requests the recording to use it as evidence to show that the staff member arrived late at work.*

There are a limited number of important exceptions to this rule[39]. The most relevant of these exceptions is when the transfer is requested by the police for the investigation or prosecution of criminal offences (see Section 10.4)

[37] Transfers can be made under Articles 7, 8 or 9 of the Regulation. These articles should be read in conjunction with other provisions of the Regulation, in particular, Articles 4, 5, 6 and 10. In addition, the recordings may also be given to the data subject to accommodate his/her right of access under Article 13 of the Regulation (see Section 12 of the Guidelines).

[38] There are certain exceptions out of this rule under Article 9(6), which provide, among others, that a transfer may be made if necessary for the "establishment of legal claims". This, in turn, should be interpreted to include requests by the police in connection with criminal investigations.

[39] See Article 20 of the Regulation.

### 10.2 *Ad hoc* and systematic transfers

Whether a transfer can be made often requires very delicate balancing between the rights of the individual and the rights or interests of those requesting the footage. Every transfer must be carefully assessed on a case by case basis.

The DPO's advice on whether the transfer is lawful under the Regulation should always be sought in case of any *ad hoc* transfer. However, if similar transfers are carried out repeatedly, the data protection assessment may also be similar. These typical transfers should be described in the Institution's video-surveillance policy. Once a policy regarding such transfers is in place, there is no need to specifically consult the DPO regarding each routine transfer, although it is always recommended to do so in case of doubt.

*Example:*

*The cameras near your main entrance also cover the adjacent bicycle parking. Once every few months the local police request a transfer of the relevant recordings to help prosecute bicycle thefts. You should have a policy in place about how to answer these requests. Then, there will be no need to consult your DPO each time.*

### 10.3 Transfers to EU investigatory bodies

Subject to the case by case analysis described above, and considering the initial purposes of the recording, the relevant footage (for example, footage that may serve as evidence), in exceptional cases, may be transferred if this is requested by

- the European Anti-fraud Office ("**OLAF**") in the framework of an investigation carried out by OLAF,
- the Commission's Investigation and Disciplinary Office ("**IDOC**") in the framework of a disciplinary investigation, under the rules set forth in Annex IX of the Staff Regulations of Officials of the European Communities, or
- those carrying out a formal internal investigation or disciplinary procedure within your Institution.

provided that it can be reasonably expected that the transfers may help investigation or prosecution of a sufficiently serious disciplinary offence or a criminal offence. No requests for data mining should be accommodated.

Management, human resources, or other persons involved should not be provided copies or otherwise allowed access to video-surveillance footage outside the above formal procedures. In case of doubt, the DPO should be consulted first.

*Example:*

*An employee files a complaint for psychological harassment against his direct superior, who, in turn, initiates a procedure for professional incompetence against his employee. Outside the framework of these procedures, the superior informally asks you to "look out" for any suspicious footage of the employee, such as visits to the office outside office hours, arriving late for work, or entering the office of others unsupervised. You should, under no circumstances, accommodate such requests.*

Finally, video-surveillance footage may also be transferred to the EDPS, for example, when the EDPS is carrying out an on-the-spot inspection or investigating a complaint.

### 10.4 Transfers to national authorities

Subject to the case by case analysis described above, and considering also the initial purposes of the recording, national police, courts, or other national authorities may, in some cases, also be given access to video-surveillance footage.

If national police, a court or other national authorities request the disclosure of recordings, the Institution should insist that a formal written request be made according to the requirements of the applicable national law regarding form and content. The Institution should only disclose the recordings if another organisation established in that country would also have been required or at least permitted to make the disclosure under similar circumstances.

Irrespective of the national requirements, whenever possible, the Institution should require a court order, a written request signed by a police officer having a sufficiently high rank, or a similar formal request. The request should specify, as closely as possible, the reason why the video-surveillance footage is needed as well as the location, date and time of the requested footage.

The Institution may, in most cases, accommodate requests from national police when the recordings are necessary to investigate or prosecute criminal offences provided that data are requested in the framework of a specific criminal investigation. However, no general requests should be accommodated for data mining purposes.

*Example:*

*A demonstration is held in front of your building involving the participation of illegal immigrants to highlight the issue of the need for regularisation of their situation. At the end of what turned out to be a peaceful demonstration with no security incidents, the national police requests that you turn over all CCTV footage you made without reference to any specific criminal investigation, and with the intention to use the footage to identify illegal immigrants and keep their images on file for any future occasion should the need arise. You should not accommodate such a request.*

Please note also that if a Member State police or other national organisation requested access in the course of an official proceeding, it would first be obliged to obtain a waiver of immunity if the footage concerned an EU staff member.

### 10.5 Register of transfers and disclosures

The Institutions should keep a register - whenever possible, in an electronic form - of transfers and disclosures. In it, each transfer to a third party should be recorded. (Third parties also include anyone within the Institution to whom a transfer is made by those having access to the recordings in the first place. This typically includes any transfer outside the security unit.) The register, in addition, should contain all instances where, although the copy of the video-surveillance footage was not transferred, third parties were shown the recordings or when the content of the recordings was otherwise disclosed to third parties.

The register should include at least the following:

- the date of the recordings,
- the requesting party (name, title and organisation),
- the name and title of the person authorising the transfer,
- a brief description of the content of the recordings,
- the reason for the request and the reason for granting it, and finally,
- whether a copy of the footage was transferred, the footage was shown, or verbal information was given.

The DPO, as well as the EDPS may require the Institution at any time to submit a copy of the register for inspection.

## 11 How to provide information to the public

### 11.1 Multi-layer approach

Information must be provided to the public about the video-surveillance in an effective and comprehensive manner[40]. The Guidelines recommend a multi-layer approach combining the following two methods:

- on-the-spot notices to immediately alert the public to the fact that monitoring takes place and provide them with essential information about the processing, and
- a detailed data protection notice posted on the Institution's intranet and internet sites for those who wish to know more (to avoid duplication of efforts, the Institution may post the public version of its video-surveillance policy on-line instead of preparing a separate data protection notice).

[40] For the list of items required by law to be included in your notice, see Article 12 of the Regulation.

These two methods can be complemented by others. For example, printed hard-copies or print-outs of the data protection notice should be made available at the reception and from the security unit upon request and the Institution should also provide a phone number and an email address for further enquiries. The availability of more detailed information on the intranet, internet (and on leaflets and via other means) must not, however, replace the on-the-spot notices.

### 11.2 On-the-spot notice

The on-the-spot notices should include a pictogram (e.g. the ISO pictogram or the pictogram customarily used where the building is located) and as much of the information listed under Article 12 of the Regulation as is reasonable under the circumstances. The notice must

- identify the "controller" (the name of the Institution is usually sufficient),
- specify the purpose of the surveillance (“for your safety and security” is usually sufficient),
- clearly mention if the images are recorded,
- provide contact information and a link to the on-line video-surveillance policy.
- If any area outside the buildings is under surveillance, this should be clearly stated. A notice in such a case merely stating that *the building* is subject to video-surveillance is misleading.

Security staff and reception must be trained on the data protection aspects of video-surveillance practices and must be able to make copies of the detailed data protection notice (video-surveillance policy) instantly available upon request. They must also be able to tell members of the public whom to contact with additional questions or to access their data.

The signs must be placed at such locations and be large enough that data subjects can notice them before entering the monitored zone and can read them without difficulty. This does not mean that a notice must be placed next to every single camera.

*Example:*

*Your Institution employs fifty people and occupies a small building in a densely built-up urban area. You may wish to put up signs of A3 size at the main entrance to the building, a slightly larger sign at the entrance to the parking lot (so that the sign would be visible from the driver’s seat), and other A3 size signs near the elevator doors in the parking lot and on the ground floor. If there are additional entrances there should be signs there as well.*

The signs within the buildings must be in the language (or languages) generally understood by staff members and most frequent visitors. Signs outside the buildings (if any areas outside are monitored) must also be posted in the local language (or languages).

If any cameras are placed at a location where those present would have a heightened expectation of privacy (see Section 6.8) or where the cameras would otherwise be unexpected and come as a surprise, an additional on-the-spot notice must be provided in the immediate vicinity of the monitored area (e.g. at the door of an individual office under surveillance)[41].

A sample on-the-spot notice is provided in Appendix 2, which Institutions may wish to customise.

### 11.3 Video-surveillance policy on-line

By adopting a video-surveillance policy and posting it on your intranet and internet sites, you also fulfil your obligation to provide a detailed data protection notice. Thus, there will be no need to draft and post a separate on-line data protection notice.

To be able to serve as an adequate data protection notice, the following information must be integrated into your video-surveillance policy in user-friendly language and format:

- identity of the controller (e.g. Institution, Directorate General, Directorate and unit)
- brief description of the coverage of the video-surveillance system (e.g. entry and exit points, computer rooms, archive rooms),
- the legal basis of the video-surveillance,
- the data collected and the purpose of the video-surveillance (any limitations on the permissible uses should also be clearly specified),
- who has access to the video-surveillance footage, and to whom the images may be disclosed,
- how the information is protected and safeguarded,
- how long the data are kept,
- how data subjects can verify, modify or delete their information (including contact information for further questions and information on how to obtain recourse in-house), and
- the right to recourse to the EDPS at any time.

In addition, the video-surveillance policy should also provide hyperlinks to:

- the EDPS Video-surveillance Guidelines,
- the Institution's audit report/s,
- the Institution's impact assessment reports/s, and
- the EDPS prior checking Opinion, where applicable.

Appendix 1 provides a sample video-surveillance policy (which may also serve as an on-line data protection notice) for a standard video-surveillance system. This policy

[41] See also Section 6.11 on covert video-surveillance.

may be customised.

### 11.4 Individual notice

Individuals must also be given individual notice if they were identified on camera (for example, by security staff in a security investigation) provided that one or more of the following conditions also apply:

- the identity of the individual is noted in any files/records,
- the video recording is used against the individual,
- the video recording is kept beyond the regular retention period,
- the video recording is transferred outside the security unit *or*
- the identity of the individual is disclosed to anyone outside the security unit.

Provisions of notice may sometimes be delayed temporarily, for example, if it is necessary for the prevention, investigation, detection and prosecution of criminal offences[42]. If such a situation arises, please seek advice from your DPO.

## 12 How to fulfil access requests by members of the public

When an individual asks what data the Institution processes about him/her, this request must be answered in a timely manner and in as much detail as it is reasonable to accommodate his/her concerns.

If the request is very general, it is usually sufficient to refer the individual to the video-surveillance policy.

*Example:*

*An individual in Member State A where your building is located emails you with the following content: "I am concerned about the video-surveillance outside your building which I pass in front of every day. Please provide me more information about the video-surveillance and the data that are processed about me." A general response referring the citizen to your video-surveillance policy will suffice.*

Other, more specific requests require a more detailed response. If this is specifically requested, access needs to be given to the recordings by allowing the individual to view the recordings or by providing a copy to him/her. In this case the rights of third parties present on the same recordings need to be carefully considered and whenever appropriate, protected (for example, by requiring consent for the disclosure or image-editing such as masking or scrambling). Protection of the rights of third parties, however, should not be used as an excuse to prevent legitimate claims of

[42] Other exceptions under Article 20 of the Regulation may apply in exceptional circumstances.

access by individuals, in particular, where recordings are used as evidence.

*Examples:*

*An employee against whom a disciplinary procedure is in progress on grounds of psychological harassment requests whether you specifically reviewed, and transferred to the management, police or other persons any video-surveillance footage related to him in connection with the procedure. If you have not done so, a simple no would suffice as an answer.*

*However, if you have made a transfer, you should say that you did, and also specify more clearly what could be seen on that footage, when and where it was recorded, and to whom and on what grounds it was transferred.*

*If he specifically so requests, and subject to the rights of others who may be seen in the same footage and the circumstances of the case, you should also allow him to view the footage transferred or provide a copy to him.*

Access to the minimum information required under Article 13 of the Regulation must be provided free of charge. Provision of access free of charge should also be a default policy for more detailed information or access to the video-surveillance recordings. However, the default policy may be changed by a reasoned decision in case the number of access requests significantly increases to discourage vexatious or frivolous requests. In this case one can start charging a *reasonable amount* for the provision of actual copies of the recordings or for allowing viewing of the recordings to help cover the costs incurred with the provision of access. The charge must not be excessive and must not serve to discourage legitimate access requests. A charge for access provision must be noted in the video-surveillance policy.

Access requests must be accommodated in a timely manner. Whenever possible, access should be provided, or, if this is not possible, another meaningful response (not merely an acknowledgement of receipt) should be given within 15 calendar days.

*Example:*

*A staff member requests access to a recording specifying the time and location of the recording. He indicates no urgency and does not specify the reason for the request and whether he wishes to obtain a copy or wants to review the recording only. Otherwise he provides all necessary information (proof of identity, photo). Within a few days of the request, you locate the recording. On the recording several other people are present in the background. Within a few more days you edit out the images of the people in the background and send an email to the staff member inviting him to schedule a meeting to come and view the images at your premises. If a swift response is given by the staff member who requested the review, the access will have been granted within 15 days.*

In more complex cases, an acknowledgement can be sent with further information regarding the cause for the delay and the expected date of further steps in the procedure. However, and irrespective of the complexity of the case, granting access (or providing a final, meaningful response rejecting the access) must not be delayed beyond the three months maximum period provided for in the Regulation[43]. In most cases, the access should be granted much earlier.

If the request is urgent, it must be answered as soon as possible and if feasible, meeting any deadlines specifically requested or apparent from the circumstances of the case.

In case of doubt as to how to respond to a particular access request, please consult the DPO. In the case of disagreement between the Institution and the individual requesting access, a simple and efficient internal review or complaint procedure should be put in place. This should be available not only to staff members, but also to third parties who request access.

The public must be informed about the review procedure both in the video-surveillance policy and in the response to the access request.

## 13 Accountability: ensuring, verifying and demonstrating good administration

Institutions must put in place polices and procedures to ensure that they use video-surveillance in compliance with the Regulation[44]. To ensure transparency and good administration, and to provide evidence of compliance to their employees, to the EDPS, and to other stakeholders[45], each Institution should verify and document the compliance of its practices with the provisions of these Guidelines.

In particular, the EDPS strongly recommends that each Institution should

- adopt a video-surveillance policy,
- carry out periodic audits and document their results in audit-reports.

In addition, in the cases referred to in Section 3.2, an impact assessment should also be carried out and documented in an impact assessment report.

[43] See Article 13 of the Regulation.

[44] Article 22(1) of the Regulation.

[45] WP Opinion 168 of 1 December 2009 on the "The Future of Privacy", referred to in footnote 13 above. See, in particular, Chapter 6 on "Strengthening Data Controllers' Responsibility".

### 13.1 Video-surveillance policy

The video-surveillance policy should

- give an overview of the video-surveillance system and describe its purposes,
- describe how the system is operated, personal data are used, and what data protection safeguards are put in place,
- explicitly confirm compliance with the Regulation and the Guidelines,
- describe any differences from the standard practices recommended in the Guidelines and explain the reasons therefore, and
- outline any necessary implementing measures.

The video-surveillance policy is a multi-purpose document and serves to meet the following needs of good administrative practice:

- Adopting this document will often be necessary to complete and specify the legal basis and thus, help establish a lawful ground for the video-surveillance[46].
- Putting existing good practices in writing and thinking through what other additional measures need to be taken are likely to improve procedures and ensure better compliance.
- Adopting a policy and making it publicly available will also help fulfil the obligation under the Regulation to provide the public with the information necessary to guarantee a fair processing.
- The policy establishes a set of rules against which compliance can be measured (e.g. during an audit).
- Finally, by increasing transparency and demonstrating compliance efforts, Institutions:
    - induce trust in their employees and in third parties;
    - help facilitate consultation with stakeholders; and
    - make interactions with the EDPS easier.

The institutions should make their video-surveillance policies publicly available on their intranet and internet sites. If this document contains confidential information, then a non-confidential version should be made publicly available.

*Examples:*

*If necessary, the security measures protecting your video-surveillance system; the detailed map with the exact camera locations and specifications; or certain specific surveillance measures relating to the fight against terrorism may be drafted in a summary fashion to ensure that the security or efficiency of the system is not jeopardised and that highly sensitive or classified information is not exposed.*

Appendix 1 provides a template for a video-surveillance policy, which the Institutions

[46] Article 5(a) of the Regulation. See also Article 8(2) of the Charter of Fundamental Rights of the European Union and related case law.

may customise.

### 13.2 Data protection audit

Each Institution should verify and document the compliance of its practices with the provisions of the Regulation, these Guidelines and its own video-surveillance policy in a data protection audit ("**audit**"). The results should be summarised in a written audit report ("**audit report**").

The objectives of the audit are twofold:

- to verify that there is a documented and up-to-date video-surveillance policy in place and that this policy complies with the Regulation and the Guidelines ("**adequacy audit**"); and
- to check that the organisation is in fact operating in accordance with is video-surveillance policy ("**compliance audit**"). This also includes verification that staff are aware of the existence of the policy, understand it, comply with its provisions and that the policy actually works and is effective.

The adequacy audit's primary concern is that there is a documented policy on how to address data protection issues and that this policy indeed adequately addresses all requirements of the Regulation and the Guidelines. The compliance audit is concerned with how the policy is being used in reality and how effective it is.

The benefits of audit include:

- it facilitates data protection compliance;
- increases data protection awareness among management and staff;
- provides input for any necessary review of the video-surveillance policy and;
- reduces the likelihood of errors leading to a complaint.

The audit report should:

- record date, scope, members of the audit team, etc.,
- summarise the main findings of the audit and any non-compliances identified,
- document suggestions for any corrective action, and
- record the nature and timescale of any agreed follow-up.

Some of the adequacy audit can be conducted off-site, based on written documentation. However, for a full audit, it is vital to also carry out on-site visits, review video-surveillance software and hardware, on-the-spot data protection notices, data retention and transfer registries, log files, access requests and other documentation available on the use of the system, and conduct interviews with management and staff members.

The audit may be carried out in house (self-audit) or an independent third party can be contracted to carry it out (third-party audit). The third party auditor may be, for example, another Institution if the auditing is carried out on a reciprocal basis. In this case, the Institutions audit each other's practices, which may encourage

benchmarking and the adoption of best practice.

Whenever possible, it should be ensured that the auditors are independent of the function being audited (typically, the security unit). The EDPS also strongly recommends that the DPO of the Institution should play a significant role in both designing and implementing the Institution's audit procedures and that he or she should be given sufficient resources to be able to do so. For self-audits, whenever possible, the EDPS recommends that the audit team should include the Institution's internal auditors and that they should receive adequate training on data protection and the Guidelines. In any event, the audit procedure must not interfere with the independence of the DPOs. The DPOs and their staff should play an active role in the audit and its follow-up, whether or not they are formally part of the audit team.

The EDPS may issue further guidance on conducting audits. This guidance may include compliance check-lists as well as further advice on audit methodology.

An audit should be done prior to the launch of the video-surveillance system but also periodically afterwards at least once every 2 years and also every time a significant change in the circumstances warrants a review. Significant system upgrades would normally warrant a review.

# 14 Outsourcing and third parties

## 14.1 Outsourcing video-surveillance

If the Institution outsources any part of its video-surveillance operations, it remains liable as a "controller". Therefore, due diligence must be exercised in choosing the contractors and a proactive approach must be taken to checking compliance.

The obligations of the processor with respect to data protection 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 Institution and the outsourced company. The outsourced company must also have a written contract with its subcontractors.

The contract, as well the tender specifications should include that the contractor should comply with the provisions of

- the Regulation,
- these Guidelines,
- the Institution's video-surveillance policy, and
- with any further advice given by the EDPS, for example, in an eventual prior checking or complaint procedure or as a result of an inspection or consultation.

The contract, as well as the tender specifications must also clearly and specifically refer to the contracted company's obligations regarding

- security,
- confidentiality, and

- its obligation to act only upon your Institution's instructions[47].

The contracted company must also provide appropriate training to its staff, including on data protection. Any direct or indirect subcontractor must be bound by the same obligations as the direct contractor. The Institution should be able to veto the choice of subcontractor, if reasonable doubts arise regarding its ability to comply with the data protection requirements.

If necessary, detailed instructions should be given to the processor to ensure that the safeguards in the Regulation and these Guidelines are respected. In this respect, particular attention should be paid to ensuring that appropriate data protection notices are given to the public and the Institution's staff.

### 14.2 Video-surveillance by third parties

At times, video-surveillance is not carried out by the Institution or a contractor on its behalf, but rather by the landlord from whom the Institution leases its premises or by a contractor on behalf of the landlord. In some cases there may be a complex contractual system involving several leases and subleases, and/or several contractors and subcontractors and the Institution may have little or no contractual influence on the operator of the video-surveillance system.

*Example:*

*Institution A may be leasing one floor in a large building from Institution B, which occupies the remaining floors of the building. Institution B, in turn, leases the premises from the owner of the building, company C. Company C outsources maintenance of the building to company D. Company D, in turn, outsources maintenance of the security of the building, including operation of a video-surveillance system, to a specialist company, Company E. In this case, there are four layers of contractual relationship between the Institution and the entity effectively carrying out the video-surveillance.*

Nevertheless, and even though in most such situations the Institution will not be considered a "controller", it should take a proactive role and make reasonable efforts to ensure that the controller carries out the video-surveillance in compliance with these Guidelines. For example, it should negotiate with the landlord (or others involved, if necessary) to ensure that important safeguards in the Regulation are respected (e.g. that on-the-spot notices are posted and more detailed information is made available on the Institution's intranet and internet sites).

## 15 Transitory provisions and future updates

The Guidelines apply to video-surveillance systems already in place as well as to systems to be installed and activities to be carried out in the future. Each Institution

[47] See Articles 22 and 23 of the Regulation.

has until 1 January 2011 to bring its existing practices into compliance with the Guidelines. Obtaining compliance for existing systems means that by this date the Institutions should

- verify what their existing practices are,
- identify what further steps are necessary to ensure full compliance, and
- implement all necessary measures to reach full compliance.

This ex-post review need not, in most cases, be a complicated and cumbersome exercise and should not, in any event, impose unnecessary administrative burdens. Indeed, many Institutions who discussed their video-surveillance systems with their DPOs in the past may find that their existing practices, to a large extent, already follow the recommendations in the Guidelines, and therefore, for the most part, all they need to do now is to verify and confirm these in writing. In addition, and importantly, verification will also allow the Institutions to identify targeted, specific adjustments to further improve their level of compliance.

In order to carry out this ex-post review in the most efficient manner, the EDPS recommends a global approach, whereby each Institution carries out a single exercise in which

- it verifies (either in a formal audit or in an informal fact-finding exercise) the adequacy and compliance of existing practices against the Regulation and the Guidelines,
- prepares (or updates) the Institution's video-surveillance policy, and finally,
- audits the revised practices against the revised policy, the Guidelines and the Regulation in a formal adequacy and compliance audit.

When necessary or helpful, an ex-post impact assessment should also be prepared as part of the same review.

### 15.1. Ex-post review of compliance status and ex-post prior checking [48]

By the same date, each DPO must notify the EDPS about the compliance status of his/her Institution. This can be done by sending a simple letter to the EDPS. The letter must

- confirm that the Institution has adopted a video-surveillance policy and
- carried out an audit;
- specify whether the Institution also carried out an impact assessment; and
- whether the Institution believes that an ex-post prior checking is necessary, and if so, on what grounds.

The following must be attached to the letter:

[48] "Ex-post" prior checking refers to checking of already existing systems, whereas a "true" prior checking under Article 27 of the Regulation refers to review of new systems (or upgrades of existing systems), which have not yet been put into place.

- the video-surveillance policy (along with its attachments),
- the audit report and
- the impact assessment report, if any.

If, despite the best efforts by an Institution, compliance on certain, specific items cannot be reached by the 1 January 2011 target date, the Institution should adopt a plan committing itself to full compliance using a step-by-step approach. The plan should explain the reasons for the delay in compliance, and identify the further steps and target dates that it plans to take to achieve full compliance as soon as possible. The plan should be submitted to the EDPS by 1 January 2011, along with the rest of the documents listed above.

Considering that these documents should already contain all the items that would normally be included in the EDPS prior checking notification form, to avoid duplication of efforts, there is no need to submit an additional prior checking notification form to the EDPS. The Institution, however, must make it clear in its letter, whether an ex-post prior-checking is requested, and if so, on what grounds. Early compliance and notification on compliance status prior to the final deadline are welcome.

If in doubt, the EDPS is available for consultation on any issues that may arise during the transition period.

As of 1 January 2011, and upon receipt of the requested documentation, the EDPS will establish a schedule for the processing of the ex-post prior checking notifications. Depending on the number and quality of the prior checking notifications received, the range of issues encountered, and other relevant factors, the EDPS may issue individual opinions or joint opinions with respect to several Institutions and/or issues. The procedure may also include on-the-spot checks or inspections.

At a subsequent stage, or parallel with processing the prior checking notifications, the EDPS may initiate enquiries and/or inspections into the practices of some or all Institutions even if these practices do not require prior checking. Depending on the level of compliance by the Institutions, the range of issues encountered, and other relevant factors, the EDPS may issue further recommendations either individually to certain Institutions or to several Institutions jointly on common issues.

### 15.2. Pending ex-post prior checking notifications

Due to the changes required by the Institutions to bring their practices into compliance with the Guidelines, the EDPS will close all ex-post prior checking procedures where the notifications were submitted prior to the publication of these Guidelines, and which were suspended pending the adoption of these Guidelines. The Institutions whose prior checking notifications have thus been closed should inform the EDPS according to the general rules and subject to the generally applicable deadline regarding their compliance status.

To assist further the compliance efforts of these Institutions, upon specific request, the EDPS may issue preliminary recommendations based on the prior checking

notification and other documents that were submitted by the Institution in the past. These recommendations will be based purely on the documentation received, without in-depth investigation.

### 15.3. Prior checking notifications for new systems

As for “true” prior checking notifications for new systems, these should be submitted as soon as possible during the planning phase, without having regard to the transitory period or the schedule established for ex-post review. The EDPS will process them as a matter of urgency.

### 15.4. Revision of the Guidelines

When significant changes in the circumstances so require, the EDPS may issue revised versions of these Guidelines. The circumstances which may trigger a revision include, among others:

- changes in video-surveillance practices within the Institutions and internationally, including technological changes,
- further development of international regulation of video-surveillance,
- lessons learnt from the application of these Guidelines, and comments received.

## Appendix 1: Sample video-surveillance policy

# [Agency] Video-surveillance Policy

Adopted by the Director's Decision on **[31 May 2010]**

### 1. Purpose and scope of the Agency's Video-surveillance Policy

For the safety and security of its buildings, assets, staff and visitors, our Agency operates a video-surveillance system. This Video-surveillance Policy, along with its attachments, describes the Agency's video-surveillance system and the safeguards that the Agency takes to protect the personal data, privacy and other fundamental rights and legitimate interests of those caught on the cameras.

### 2. How do we ensure that our video-surveillance system is designed with privacy and data protection concerns in mind and is compliant with data protection law?

**2.1. Revision of the existing system.** A video-surveillance system had already been operating in our Agency before the issuance of the Video-Surveillance Guidelines by the European Data Protection Supervisor ("**Guidelines**") on _____ 2010. Our procedures, however, have since then been revised to comply with the recommendations set forth in the Guidelines (Guidelines, Section 15). **[hyperlink to the Guidelines at the EDPS website]**

**2.2. Compliance status.** The Agency processes the images in accordance with both the Guidelines and Regulation (EC) No 45/2001 on the protection of personal data by the Community institutions and bodies. **[If you deviate from any recommendations in the Guidelines, this should be clearly stated and justified in your video-surveillance policy.]**

**2.3. Self-audit.** The system was subject to a self-audit. **The audit report** is attached as **Attachment 1.**

**2.4. Notification of compliance status to the EDPS.** Considering the limited scope of the system, it was not necessary to carry out a formal impact assessment (Guidelines, Section 3.2) or to submit a prior checking notification to the EDPS (Guidelines, Section 4.3). **[Note that in case an impact assessment has been carried out, your impact assessment report should also be attached to your video-surveillance policy and the main issues and findings must be highlighted in the policy itself. Similarly, if a prior checking opinion is issued by the EDPS, this should also be attached, and the main EDPS recommendations and your follow-up on those recommendations should be summarised in the policy itself.]**

Simultaneously with adopting this Video-surveillance Policy, we also notified the EDPS of our compliance status by sending them a copy of our Video-surveillance Policy and our first audit report.

**2.5. Contacts with the relevant data protection authority in the Member State.** The competent data protection authority in **[insert country]** was informed and its concerns and recommendations were taken into account. In particular, both the on-the-spot notice and this Video-surveillance Policy are also available in **[local language/s].**

**2.6. Director's decision and consultation.** The decision to use the current video-surveillance system and to adopt the safeguards as described in this Video-surveillance Policy was made by the Director of the Agency after consulting

- the head of the Agency's security unit,
- the Agency's Data Protection Officer,
- and the Staff Committee.

During this decision-making process, the Agency

- demonstrated and documented the need for a video-surveillance system as proposed in this policy,
- discussed alternatives and concluded that the maintenance of the current video-surveillance system, after the adoption of the data protection safeguards proposed in this policy, is necessary and proportionate for the purposes described in Section 1 (see Guidelines, Section 5), and
- addressed the concerns of the DPO and the Staff Committee (see Guidelines, Section 4).

**2.7 Transparency.** The Video-surveillance Policy has two versions, a version for restricted use and this public version available and posted on our internet and intranet sites at **[internet and intranet addresses]**. This public version of the Video-surveillance Policy may contain summary information with respect to particular topics or attachments. When this is the case, it is always clearly stated. Information is only omitted from the public version when the preservation of confidentiality is absolutely necessary for compelling reasons (e.g. for security reasons or to preserve the confidentiality of commercially sensitive information or to protect the privacy of individuals).

**2.8. Periodic reviews.** A periodic data protection review will be undertaken by the security unit every two years, the first by 31 May 2012. During the periodic reviews we will re-assess that:

- there continues to be a need for the video-surveillance system,
- the system continues to serve its declared purpose, and that
- adequate alternatives remain unavailable.

The periodic reviews will also cover all other issues addressed in the first report, in particular, whether our Video-Surveillance Policy continues to comply with the Regulation and the Guidelines (adequacy audit), and whether it is followed in practice (compliance audit). Copies of the periodic reports will also be attached to this Video-surveillance Policy in **Attachment 1**.

**2.9. Privacy-friendly technological solutions.** We also implemented the following privacy-friendly technological solutions (see Guidelines, Section 3.4):

**[list and describe the solutions implemented]**

**3. What areas are under surveillance?**

The video-surveillance system consists of **[seven fixed cameras]. A map with the locations of the cameras** is included in **Attachment 2.**

Of the **[seven cameras, six]** are located at entry and exit points of our building, including the main entrance, emergency and fire exits and the entrance to the parking lot. In addition, there is also a camera at the entrance to the stairway in the parking lot.

There are no cameras elsewhere either in the building or outside of it. We also do not monitor any areas under heightened expectations of privacy such as individual offices, leisure areas, toilet facilities and others (see Guidelines, Section 6.8). The location of the cameras was carefully reviewed to ensure that they minimise the monitoring of areas that are not relevant for the intended purposes (Guidelines, Section 6.1).

Monitoring outside our building on the territory of **[insert name of the Member State where you are located]** is limited to an absolute minimum, as recommended in Section 6.5 of the Guidelines.

**4. What personal information do we collect and for what purpose?**

**4.1. Summary description and detailed technical specifications for the system.** The video-surveillance system is a conventional static system. It records digital images and is equipped with motion detection. It records any movement detected by the cameras in the area under surveillance, together with time, date and location. All cameras operate 24 hours a day, seven days a week. The image quality in most cases allows identification of those in the camera's area of coverage (see Guidelines, Section 6.4). The cameras are all fixed (there are no pan-tilt-and-zoom cameras), and thus, they cannot be used by the operators to zoom in on a target or follow individuals around.

We do not use high-tech or intelligent video-surveillance technology (see Section 6.9 of the Guidelines), do not interconnect our system with other systems (Section 6.10), and we do not use covert surveillance (Section 6.11), sound recording, or "talking

CCTV" (Section 6.12). **The technical specifications for** the cameras and **for the video-surveillance system as a whole** (including any software and hardware) are included in **Attachment 3.**

**4.2. Purpose of the surveillance.** The Agency uses its video-surveillance system for the sole purposes of security and access control. The video-surveillance system helps control access to our building and helps ensure the security of our building, the safety of our staff and visitors, as well as property and information located or stored on the premises. It complements other physical security systems such as access control systems and physical intrusion control systems. It forms part of the measures to support our broader security policies and helps prevent, deter, and if necessary, investigate unauthorised physical access, including unauthorised access to secure premises and protected rooms, IT infrastructure, or operational information. In addition, video-surveillance helps prevent, detect and investigate theft of equipment or assets owned by the Agency, visitors or staff, and threats to the safety of visitors or personnel working at the office (e.g. fire, physical assault).

**4.3. Purpose limitation.** The system is not used for any other purpose, for example, it is not used to monitor the work of employees or to monitor attendance. Neither is the system used as an investigative tool (other than investigating physical security incidents such as thefts or unauthorised access) It is only in exceptional circumstances that the images may be transferred to investigatory bodies in the framework of a formal disciplinary or criminal investigation as described in Section 6.5 below (see Sections 5.7, 5.8 and 10.3 of the Guidelines).

**4.4. No *ad hoc* surveillance foreseen.** We foresee no *ad hoc* surveillance operations for which we would need to plan at this time (see Guidelines, Section 3.5).

**4.5. Webcams.** We have no webcams (see Section 5.10 of the Guidelines).

**4.6. No special categories of data collected.** We collect no special categories of data (Section 6.7 of the Guidelines).

**5. What is the lawful ground and legal basis of the video-surveillance?**

The use of our video-surveillance system is necessary for the management and functioning of our Agency (for the security and access control purpose described in Section 4.2 above). Therefore, we have a lawful ground for the video-surveillance (see Section 5.2 of the Guidelines). A more detailed and specific legal basis for the video-surveillance is provided in this Video-surveillance Policy. This policy, in turn, forms part of the broader security policies adopted by our Agency.

**6. Who has access to the information and to whom is it disclosed?**

**6.1. In-house security staff and outsourced security-guards.** Recorded video is accessible to our in-house security staff only. Live video is also accessible to security guards on duty. These security guards work for an out-sourced security company. The **contract with this security company** is included in **Attachment 4.**

**6.2. Access rights.** The Agency's Security Policy for Video-surveillance (see Section 7 below and Attachment 7) clearly specifies and documents who has access to the video-surveillance footage and/or the technical architecture of the video-surveillance system, for what purpose and what those access rights consist of. In particular, the document specifies who has the right to:

- view the footage real-time,
- view the recorded footage, or
- copy,
- download,
- delete, or
- alter any footage.

**6.3. Data protection training.** All personnel with access rights, including the outsourced security guards, were given their first data protection training on **[15 May 2010].** Training is provided for each new member of the staff and periodic workshops on data protection compliance issues are carried out at least once every two years for all staff with access rights (see Section 8.2 of the Guidelines).

**6.4. Confidentiality undertakings.** After the training each staff member also signed a confidentiality undertaking. This undertaking was also signed by the outsourced company. Copies of these **confidentiality undertakings** are attached as **Attachment 5** (see Section 8.3 of the Guidelines).

**6.5. Transfers and disclosures.** All transfers and disclosures outside the security unit are documented and subject to a rigorous assessment of the necessity of such transfer and the compatibility of the purposes of the transfer with the initial security and access control purpose of the processing (see Section 10 of the Guidelines). **The register of retention and transfers** is included in **Attachment 6** (see Section 10.5 and 7.2 of the Guidelines). The DPO of the Agency is consulted in each case. **[If you have routine transfers which are made without the involvement of the DPO, please describe your policy in detail in this Video-surveillance Policy.]**

No access is given to management or human resources. **[If this is not the case, please provide illustrative examples of such transfers. Please also describe your rules on what can be transferred to whom and under what circumstances.]**

Local police may be given access if needed to investigate or prosecute criminal offences. There were a few occasions in the past where police were given access to footage to help investigate bicycle theft from the bicycle racks located at the entrance to the garage. On no other occasion was access given to the police for the past **[five years]** for which we hold records of transfers. **[Again, if there were other cases, please provide illustrative examples of such transfers. Please also describe your rules on what can be transferred to whom and under what circumstances.]**

Under exceptional circumstances, access may also be given to

- the European Anti-fraud Office ("**OLAF**") in the framework of an investigation carried out by OLAF,
- the Commission's Investigation and Disciplinary Office ("**IDOC**") in the framework of a disciplinary investigation, under the rules set forth in Annex IX of the Staff Regulations of Officials of the European Communities, or
- those carrying out a formal internal investigation or disciplinary procedure within the Institution,

provided that it can be reasonably expected that the transfers may help investigation or prosecution of a sufficiently serious disciplinary offence or a criminal offence. No requests for data mining are accommodated. For the past **[five years]** for which we hold records of transfers, we have not authorised a transfer under any of the above grounds.

**7. How do we protect and safeguard the information?**

In order to protect the security of the video-surveillance system, including personal data, a number of technical and organisational measures have been put in place. These are detailed in a processing-specific security policy ("**Security Policy for Video-surveillance**"), which is attached as **Attachment 7**.

The Agency's Security Policy for Video-surveillance was established in accordance with Section 9 of the EDPS Video-surveillance Guidelines.

Among others, the following measures are taken:

- Secure premises, protected by physical security measures, host the servers storing the images recorded; network firewalls protect the logic perimeter of the IT infrastructure; and the main computer systems holding the data are security hardened.
- Administrative measures include the obligation of all outsourced personnel having access to the system (including those maintaining the equipment and the systems) to be individually security cleared.
- All staff (external and internal) signed non-disclosure and confidentiality agreements.
- Access rights to users are granted to only those resources which are strictly necessary to carry out their jobs.
- Only the system administrator specifically appointed by the controller for this purpose is able to grant, alter or annul any access rights of any persons. Any provision, alteration or annulment of access rights is made pursuant to the criteria established in the Security Policy for Video-surveillance (see Attachment 7).
- The Security Policy for Video-surveillance contains an up-to-date list of all persons having access to the system at all times and describes their access rights in detail.

**8. How long do we keep the data?**

The images are retained for a maximum of 48 hours. Thereafter, all images are deleted. If any image needs to be stored to further investigate or evidence a security incident, they may be retained as necessary. Their retention is rigorously documented and the need for retention is periodically reviewed. A copy of the **register of retention and transfers** is included in **Attachment 6** (see Section 7 of the Guidelines.)

The system is also monitored live by the security guard in the downstairs building reception 24 hours a day.

**9. How do we provide information to the public?**

**9.1. Multi-layer approach.** We provide information to the public about the video-surveillance in an effective and comprehensive manner (see Guidelines, Section 11). To this end, we follow a multi-layer approach, which consists of a combination of the following two methods:

- on-the-spot notices to alert the public to the fact that monitoring takes place and provide them with essential information about the processing, and
- we post this Video-surveillance Policy on our intranet and also on our internet sites for those wishing to know more about the video-surveillance practices of our Institution.

Print-outs of this Video-surveillance Policy are also available at our building reception desk and from our security unit upon request. A phone number and an email address are provided for further enquiries.

We also provide on-the-spot notice adjacent to the areas monitored. We placed a notice near the main entrance, the elevator entrance in the parking lot and at the entry to the parking lot.

The Agency's on-the-spot data protection notice is included as **Attachment 8.**

**9.2. Specific individual notice.** In addition, individuals must also be given individual notice if they were identified on camera (for example, by security staff in a security investigation) provided that one or more of the following conditions also apply:

- their identity is noted in any files/records,
- the video recording is used against the individual,
- kept beyond the regular retention period,
- transferred outside the security unit, *or*
- if the identity of the individual is disclosed to anyone outside the security unit.

Provision of notice may sometimes be delayed temporarily, for example, if it is necessary for the prevention, investigation, detection and prosecution of criminal

offences[49]. The Institution's DPO is consulted in all such cases to ensure that the individual's rights are respected.

**10. How can members of the public verify, modify or delete their information?** Members of the public have the right to access the personal data we hold on them and to correct and complete such data. Any request for access, rectification, blocking and/or erasing of personal data should be directed to Ms/Mr _____, Head of Unit __ **[email address and telephone number].** He or she may also be contacted in case of any other questions relating to the processing of personal data.

Whenever possible, the security unit responds to an enquiry in substance within 15 calendar days. If this is not possible, the applicant is informed of the next steps and the reason for the delay within 15 days. Even in the most complex of cases access must be granted or a final reasoned response must be provided rejecting the request within three months at the latest. The unit must do its best to respond earlier, especially if the applicant establishes the urgency of the request.

If specifically requested, a viewing of the images may be arranged or the applicant may obtain a copy of the recorded images on a DVD or other media. In case of such a request, the applicants must indicate their identity beyond doubt (e.g. they should bring identity cards when attending the viewing) and, whenever possible, also designate the date, time, location and circumstances when they were caught on cameras. They must also provide a recent photograph of themselves that allows the security staff to identify them from the images reviewed.

At this time, we do not charge applicants for requesting a viewing or a copy of their recorded images. However, we reserve the right to charge a reasonable amount in case the number of such access requests increases.

An access request may be refused when an exemption under Article 20(1) of Regulation 45/2001 applies in a specific case. For example, following a case-by-case evaluation we may have to conclude that restricting access may be necessary to safeguard the investigation of a criminal offence. A restriction may also be necessary to protect the rights and freedoms of others, for example, when other people are also present on the images, and it is not possible to acquire their consent to the disclosure of their personal data or to use image-editing to remedy the lack of consent.

**11. Right of recourse**

Every individual has the right of recourse to the European Data Protection Supervisor (edps@edps.europa.eu) if they consider that their rights under Regulation 45/2001 have been infringed as a result of the processing of their personal data by the Agency. Before doing so, we recommend that individuals first try to obtain recourse by contacting:

[49] Other exceptions under Article 20 of the Regulation may also apply in exceptional circumstances.

- the head of the security unit (see contact details above), and/or
- the data protection officer of the Agency **[insert name, telephone number and email address]**

Staff members may also request a review from their appointing authority under Article 90 of the Staff Regulation.

**[Details of internal recourse procedure, including timelines and contact details.]**

* * *

**Attachments to the Video-surveillance Policy:**

- **The audit report** is attached as **Attachment 1.** Attachment 1 will also contain the **periodic reviews.**
- A map with the locations of the cameras is included in **Attachment 2**.
- The **technical specifications** for the cameras and for the video-surveillance system as a whole (including any software and hardware) are included in **Attachment 3**.
- The **contract with the outsourced security company** is included in **Attachment 4**.
- Copies of the **confidentiality undertakings** are attached as **Attachment 5** (see Section 8.3 of the Guidelines).
- **The register of retention and transfers** is included in **Attachment 6** (see Sections 10.5 and 7.2 of the Guidelines).
- In order to protect the security of the video-surveillance system, including personal data contained in it, a number of technical and organisational measures have been put in place. These are detailed in a processing-specific security policy ("**Security Policy for Video-surveillance**"), which is attached as **Attachment 7**.
- The Agency's **on-the-spot data protection notice** is included as **Attachment 8.**

## Appendix 2: Sample on-the-spot data protection notice

**[Insert your video-surveillance pictogram: you may consider, for example, the ISO pictogram or the pictogram customarily used where you are located.]**

For your safety and security, this building and its immediate vicinity is under video-surveillance. No images are recorded. **[Alternative: The recordings are retained for 48 hours.]**

For further information, please consult www.domainnameofyourinstitution/cctv or contact the Agency's security unit at **[telephone number and email address].**

**[Include multiple language versions when applicable.]**