



GIOVANNI BUTTARELLI
ASSISTANT SUPERVISOR

Data Protection Officers of European
Community institutions and bodies

Brussels, 7 July 2009
GB/ZB/ktl D(2009)954 C 2006-0291

Subject: Notice of consultation on the EDPS Video-surveillance Guidelines

Dear colleagues,

I am pleased to provide you with the consultation draft of the EDPS Video-surveillance Guidelines, for your review and comments. A summary introducing the compliance framework proposed by the Guidelines is set forth in an annex to this letter. A copy of this consultation version along with this letter and the summary is also publicly available on the EDPS website at www.edps.europa.eu.

I would be grateful if you could circulate the draft as widely as possible within your institution, in particular to key stakeholders such as

- § the management of your institution,
- § all those directly responsible for video-surveillance within your organization (this usually includes the head of your security unit but there may be other actors, too), and
- § your Staff Committee.

You may also circulate the draft to "processors" and other actors outside your institutions, for example, to outsourced CCTV operating companies or contractors who supplied your CCTV system or are responsible for its technical maintenance.

Deadline for written comments: 15 September 2009

I would be grateful if you could provide any written comments on the Guidelines by 15 September 2009. (To help us with our planning, if you can, please also let us know by 22 July 2009 whether you intend to comment.) Please send your comments to Zsuzsanna Belenyessy at zsuzsanna.belenyessy@edps.europa.eu with a copy to the EDPS general email-box at edps@edps.europa.eu. In the subject line please write "Comments on the draft EDPS video-surveillance Guidelines, EDPS ref nr 2006-291" and the name of your organization. Please also advise accordingly any stakeholders who wish to comment separately.

Workshop on 30 September 2009

It is our intention to discuss these Guidelines in a workshop in the afternoon of 30 September 2009 in Brussels and formally issue the Guidelines shortly afterwards during the autumn of 2009. Please reserve the date (which, for convenience, is directly preceding the date of the October DPO meeting) in your calendar.

While we wish to keep the number of participants manageable to maximize the effectiveness of the workshop, it would be helpful if, in addition to Data Protection Officers, at least a few security officials, IT specialists and Staff Committee representatives also attended, especially, but not exclusively, from some of the larger institutions. Therefore, in case of interest, please feel free to propose attendance by such colleagues (please no more than two or three participants per any Institution/Agency). The language of the workshop will be English.

To help us organize the workshop, please send Zsuzsanna Belenyessy (with a copy to the general EDPS email-box) a short note confirming who plans to attend the workshop from your organization (name and function/title). Please do so at your earliest convenience but in any event no later than 22 July 2009. As noted above, if you can, please also inform us by this date whether you plan to submit any written comments later on. Finally, please also indicate if there are any topics that are of particular interest to you and that you wish to discuss in more detail at the workshop. The draft agenda will be prepared taking this information into account.

Further information regarding the workshop, including time, location and draft agenda will be circulated in due course.

We thank you for your cooperation and look forward to receiving your comments, and meeting you at the workshop dedicated to the EDPS Video-surveillance Guidelines on 30 September 2009.

(Signed)

Giovanni BUTTARELLI

Enclosures :

1. Annex 1: A summary introducing the compliance framework proposed by the Guidelines
2. Annex 2: Consultation draft of the Guidelines



C 2006-0291

Summary introducing the compliance framework proposed by the EDPS Video-surveillance Guidelines

7 July 2009

Purpose and scope of the Guidelines. The EDPS plans to issue these Guidelines with the dual purpose of (i) contributing to the prevention of the uncontrolled proliferation of video-surveillance in cases where the use of this technology is not warranted and (ii) assisting the Community institutions and bodies ("**Institutions**") in using video-surveillance responsibly and with effective safeguards in place in those cases when the use of video-surveillance is justified.

The Guidelines aim at providing practical advice rather than legal theory. They are intended to be flexible but also to give certainty to the Institutions as to what uses of video-surveillance the EDPS is likely to find objectionable; what steps the Institutions need to take before they install a video-surveillance system or update an existing one; and what measures they need to take on an on-going basis to ensure that data protection concerns continue to be adequately addressed during the operation of the system.

Topics addressed in the Guidelines. More specifically, the Guidelines recommend the Institutions to clearly establish the purposes they wish to achieve with the system; to carefully analyze whether video-surveillance technology is an efficient and proportionate means to achieve this purpose; to look for alternative solutions before deciding to use cameras; and to work together with the Data Protection Officers ("**DPO**")s of the Institutions to decide where to site cameras, how to use them, and what safeguards to introduce to help protect the privacy and other legitimate interests or fundamental rights of the individuals captured on the cameras.

The Institutions are also required to keep the video-footage no longer than necessary; strictly limit the range of recipients of the footage; document any use and transfer of the video-footage; and take security measures to minimize the risk of unauthorized access. In addition, the Institutions are also required to provide a meaningful notice to the public. The EDPS encourages a multi-layer approach for notice provision, which should include, in addition to signs on the spot, more detailed information on the website of the Institution and provision of similar detailed information in leaflets or in print-outs upon request. Each Institution is also required to set up a mechanism to accommodate access requests from members of the public who wish to know what video-data are being processed about them.

Procedural framework for compliance. The Guidelines provide detailed guidance to smaller Institutions, among them many agencies with relatively simple, static and standard video-surveillance systems. However, certain complex, novel or intrusive systems (e.g. dynamic-preventive CCTV systems or CCTV systems linked to

Postal address: rue Wiertz 60 - B-1047 Brussels

Offices: rue Montoyer 63

E-mail : edps@edps.europa.eu - Website: www.edps.europa.eu

Tel.: 02-283 19 00 - Fax : 02-283 19 50

biometric databases) require additional safeguards, which can be developed with the assistance of the EDPS who will review the additional issues posed by such systems in a prior checking procedure and provide additional recommendations.

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 will have six months as of the date of publication, to bring its existing practices in line with the recommendations contained in the Guidelines.

By the end of that period, each DPO should notify the EDPS about the compliance status of his/her Institution. This can be done by sending a simple letter to the EDPS

- § confirming that the Institution adopted a video-surveillance policy (see Section 13.1) and
- § carried out a self-audit or third-party audit (see Section 13.2);
- § specifying whether the Institution also carried out a privacy and data protection impact assessment (Section 3.2) with respect to any particular issue/s; and
- § informing the EDPS whether based on the findings of the data protection compliance report, and the privacy and data protection impact assessment, the Institution believes that an ex-post prior checking is necessary with respect to any particular issue/s.

A copy of the video-surveillance policy (along with its attachments) as well as a copy of the data protection compliance report and the impact assessment report (if any) should be attached to the letter.

After the lapse of the six month deadline, 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. If necessary, the procedure may also include on-the-spot 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.

Best practices. The Guidelines focus only on issues relevant to the Institutions. However, when developing these Guidelines, the EDPS took into account not only the institutional experience accumulated so far, but also best practices in Member States and internationally.

Future updates. As and when required, the Guidelines will be updated in the future.

THE EDPS VIDEO-SURVEILLANCE GUIDELINES

Table of contents

FOREWORD BY THE EUROPEAN DATA PROTECTION SUPERVISOR (“EDPS”).....	4
1 OBJECTIVE OF THE GUIDELINES: A PRACTICAL GUIDE TOWARDS COMPLIANCE.....	5
2 WHAT THESE GUIDELINES COVER	5
2.1 SCOPE OF THE GUIDELINES	5
2.2 VIDEO-SURVEILLANCE FOR PURPOSES OF SECURITY AND ACCESS CONTROL.....	6
2.3 VIDEO-SURVEILLANCE FOR PURPOSES OTHER THAN SECURITY AND ACCESS CONTROL.....	7
2.4 EXCLUSIONS FROM THE SCOPE OF THE GUIDELINES.....	7
2.5 FURTHER CLARIFICATIONS ON THE SCOPE OF THE GUIDELINES	8
3 “PRIVACY BY DESIGN”	11
3.1 DATA PROTECTION AS AN INTEGRAL PART OF PROJECT PLANNING AND IMPLEMENTATION.....	11
3.2 “PRIVACY AND DATA PROTECTION IMPACT ASSESSMENT”	11
3.3 PRIVACY-FRIENDLY TECHNOLOGICAL SOLUTIONS	13
3.4 CONSULTATION OF STAKEHOLDERS AND COMPETENT AUTHORITIES	14
3.5 VERIFICATION AND DOCUMENTATION OF COMPLIANCE	14
3.6 TIMELY PLANNING FOR <i>AD HOC</i> SURVEILLANCE OPERATIONS	14
4 WHO SHOULD BE CONSULTED ABOUT THE NEW SYSTEM?	15
4.1 INVOLVEMENT AND ROLE OF THE DPO.....	15
4.2 CONSULTATION WITH THE STAFF COMMITTEE AND OTHER STAKEHOLDERS.....	15
4.3 PRIOR CHECKING BY THE EDPS.....	16
4.4 INVOLVEMENT OF NATIONAL DATA PROTECTION AUTHORITIES	16
5 DECIDING WHETHER TO USE VIDEO-SURVEILLANCE.....	17
5.1 WHAT ARE THE BENEFITS TO BE GAINED FROM THE USE OF VIDEO-SURVEILLANCE? IS THE PURPOSE OF THE SYSTEM CLEARLY SPECIFIED, EXPLICIT AND LEGITIMATE?.....	18
5.2 DOES THE INSTITUTION HAVE A LAWFUL GROUND FOR THE VIDEO-SURVEILLANCE?.....	19
5.3 IS THE NEED TO USE VIDEO-SURVEILLANCE CLEARLY DEMONSTRATED?	19
5.4 IS VIDEO-SURVEILLANCE AN EFFICIENT TOOL TO ACHIEVE ITS INTENDED PURPOSE?	20
5.5 ARE LESS INTRUSIVE ALTERNATIVES AVAILABLE?	20
5.6 DO THE BENEFITS GAINED FROM VIDEO-SURVEILLANCE OUTWEIGH ITS DETRIMENTAL EFFECTS?	21
5.7 EMPLOYEE MONITORING.....	22
5.8 WEBCAMS.....	23

6	SELECTING, SITING AND CONFIGURING YOUR VIDEO-SURVEILLANCE SYSTEM.....	23
6.1	CAMERA LOCATIONS AND VIEWING ANGLES.....	23
6.2	NUMBER OF CAMERAS	24
6.3	TIMES OF MONITORING	25
6.4	RESOLUTION AND IMAGE QUALITY	25
6.5	MONITORING ON MEMBER STATE TERRITORY	25
6.6	MONITORING IN THIRD COUNTRIES	27
6.7	SPECIAL CATEGORIES OF DATA	27
6.8	AREAS UNDER HEIGHTENED EXPECTATIONS OF PRIVACY.....	28
6.9	HIGH-TECH AND/OR INTELLIGENT VIDEO-SURVEILLANCE.....	29
6.10	INTERCONNECTION OF VIDEO-SURVEILLANCE SYSTEMS	29
6.11	COVERT SURVEILLANCE	30
6.12	SOUND RECORDING AND “TALKING CCTV”	31
7	HOW LONG CAN THE RECORDINGS BE KEPT?	31
7.1	RETENTION PERIOD.....	31
7.2	REGISTER OF RECORDINGS RETAINED BEYOND THE RETENTION PERIOD	33
8	WHO SHOULD HAVE ACCESS TO THE IMAGES?.....	34
8.1	A SMALL NUMBER OF CLEARLY IDENTIFIED INDIVIDUALS ON A NEED-TO-KNOW BASIS	34
8.2	DATA PROTECTION TRAINING	36
8.3	CONFIDENTIALITY UNDERTAKINGS.....	36
9	WHAT SECURITY MEASURES SHOULD BE TAKEN TO PROTECT THE DATA?.....	36
10	TRANSFERS IN-HOUSE AND OUTSIDE THE INSTITUTION.....	38
10.1	GENERAL FRAMEWORK FOR TRANSFERS.....	38
10.2	THE ROLE OF THE DPO: <i>AD HOC</i> AND SYSTEMATIC OR REPEAT TRANSFERS	39
10.3	TRANSFERS TO EU INVESTIGATORY BODIES	40
10.4	TRANSFERS TO NATIONAL AUTHORITIES.....	40
10.5	REGISTER OF TRANSFERS AND DISCLOSURES	41
11	HOW TO PROVIDE INFORMATION TO THE PUBLIC.....	42
12	HOW TO FULFIL ACCESS REQUESTS BY MEMBERS OF THE PUBLIC.....	44
13	MAINTAINING, VERIFYING AND DOCUMENTING GOOD ADMINISTRATION	46
13.1	VIDEO-SURVEILLANCE POLICY	47
13.2	DATA PROTECTION COMPLIANCE REPORT	47
14	OUTSOURCING AND VIDEO-SURVEILLANCE BY OTHER THIRD PARTIES.....	48
14.1	OUTSOURCING VIDEO-SURVEILLANCE	48

14.2	VIDEO-SURVEILLANCE BY OTHER THIRD PARTIES	48
15	TRANSITORY PROVISIONS AND FUTURE UPDATES	49
	APPENDIX 1: FURTHER INFORMATION ON PRIOR CHECKING BY THE EDPS.....	52
	APPENDIX 2: SAMPLE VIDEO-SURVEILLANCE POLICY FOR A SMALL VIDEO-SURVEILLANCE SYSTEM	56
	APPENDIX 3: SAMPLE ON-THE-SPOT DATA PROTECTION NOTICE	65
	APPENDIX 4: SAMPLE ON-LINE DATA PROTECTION NOTICE	66

Foreword by the European Data Protection Supervisor (“EDPS”¹)

¹ PM. The Foreword will be included in the final version only.

1 Objective of the guidelines: a practical guide towards compliance

These guidelines ("**Guidelines**") were issued by the 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 bodies² ("**Regulation**").

The objective of the Guidelines is to offer practical guidance to the Community institutions and bodies ("**Institutions**") operating video-surveillance equipment on how to comply with the provisions of 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 minimizes impact on privacy and other fundamental rights.

The Guidelines are addressed to those within the Institutions who are in the position to decide whether to install video-surveillance systems and are ultimately responsible for their operation (the "**controllers**" in data protection terms³). This typically includes the heads of the security units of the Institutions but also the management of the Institutions ultimately responsible for strategic decision-making regarding the installation and use of video-surveillance systems. The Guidelines also aim at providing useful information to outside contractors assisting in the installation and operation of the systems (some of them acting as "**processors**"⁴), as well as to the Institutions' data protection officers ("**DPOs**")⁵, staff members, their representatives and visitors to the buildings or those within their vicinity.

The Guidelines are not definitive statements of law. Instead, they offer recommendations and suggest best practices, while acknowledging that there may always be exceptions to the rule where a case-by-case analysis is necessary.

2 What these Guidelines cover

2.1 Scope of the Guidelines

The Guidelines are applicable to video-surveillance carried out by the Institutions or on their behalf if the cameras capture personal data as defined in the Regulation. Further clarifications on the scope of the Guidelines are set forth below.

² 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.

³ See Article 2(d) of the Regulation.

⁴ See Article 2(e) of the Regulation.

⁵ See Article 24 of the Regulation.

2.2 Video-surveillance for purposes of security and access control

The Institutions typically use video-surveillance for security and access control. They usually specify the purpose of their video-surveillance systems as helping to control access and to ensure the safety and security of their buildings and property, people and information on the premises.

The primary purpose is usually stated as the *prevention* of security incidents. In practice, however, rather than preventing security incidents, video-surveillance often merely serves to *deter* the occurrence of such incidents or to *investigate* them after the fact, and *secure evidence*, should such incidents occur.

With that said, deterrence or investigation of security incidents and the securing of evidence of security incidents may be legitimate *complementary* goals to the *primary* goal of prevention, and as such, may come within the definition of security purpose.

However, it should be emphasised that the security purposes should not, in any event, be defined to include the investigation of facts other than security incidents (e.g. investigation of benefit fraud, professional incompetence, psychological harassment or procurement fraud).⁶

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 at the building reception. The cameras also record the footage. At 4 am, the alarm system rings signalling unauthorized 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 within the scope of the security purpose.

This is not the case where the investigation is not triggered by a security incident. Using the CCTV system for investigating the activities of Mr. X, an official at your Institution who is suspected of having committed procurement fraud would go beyond the security and access control purpose.

As they constitute the most common purpose for video-surveillance within the Institutions, the Guidelines focus primarily on the safeguards necessary for video-surveillance for security and access control purposes. However, the Guidelines are also relevant and applicable to any other type of video-surveillance.

⁶ For more information of what may be considered as a legitimate purpose of your video-surveillance system, please see Section 5.1.

2.3 Video-surveillance for purposes other than security and access control

The EDPS discourages the proliferation of video-surveillance for other purposes, including, among others, for purposes of employee monitoring or internal investigations (except when directly related to a security incident, as noted in Section 2.2 above). However, it cannot be excluded that in exceptional circumstances, video-surveillance technology might nevertheless also be used for purposes other than security and access control.

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, any such proposed video-surveillance is subject to privacy and data protection impact assessment by the Institution as described in Section 3.2 below. In some cases (including the case of employee monitoring and internal investigations) the proposed system must also be submitted for prior checking to the EDPS.⁷

2.4 Exclusions from the scope of the Guidelines

The Guidelines do not apply to

- § video-phone calls and video-conferencing,
- § simple video-entry systems without recording⁸
- § camera use for artistic or journalistic purposes (such as for film making or to record or broadcast newsworthy events)⁹,
- § 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 camera 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.

⁷ Regarding prior checking by the EDPS, please see Article 27 of the Regulation. See also Section 4.3 and Appendix 1 of these Guidelines for more detail.

⁸ By this we mean a simple system which allows a receptionist or security guard to remotely open a closed door (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 2.5.4 below.

⁹ 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.

2.5 Further clarifications on the scope of the Guidelines

2.5.1. What does video-surveillance mean? Does it only include CCTV systems?

For purposes of these Guidelines, video-surveillance is defined as the systematic¹⁰ visual monitoring of a specific area, event, activity, or person by means of any 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 video-data. This includes, for example, any type of portable video-cameras or any cameras taking still images and all webcams.

2.5.2. What constitutes personal data?

Personal data are 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."¹¹ What does this mean in practice?

First, recognizable 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 recognizable facial images which are capable of identifying the perpetrator in case of unauthorized access. The Guidelines apply even if you only recorded the images and never reviewed the recordings.

However, there is often no need to capture recognizable facial images for the

¹⁰ The monitoring does not need to be continuous or permanent to be considered systematic. See, e.g. Section 2.5.3 below. Note also that even if an Institution considers that a particular type of monitoring is not systematic, and thus, it is not falling under these Guidelines, the monitoring may still fall under the Regulation, and therefore, may still require appropriate data protection safeguards. For these systems, compliance needs must be assessed by the Institutions on a case by case basis.

¹¹ 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.

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:

The 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 recognizable facial images, following a serious incident, police, after extensive research, may be able to indirectly identify the persons captured on the cameras by 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). The Guidelines apply.

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 license plates, is further connected to a database containing license plate registration data. It is also equipped with software capable of reading number plates and matching those with the person in whose name the car 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, as a matter of fact, 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.

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

No, any video-surveillance comes under the scope of these Guidelines even if the

cameras are used only 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.

2.5.4. If a video-surveillance system does not record any footage does it still come under the Guidelines?

Yes, not only recording but also live video-monitoring or live video-broadcast come under the scope of the Regulation, and also 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 are present even if no footage is recorded and the footage is only transferred to the intended recipients via an internal network. The risks include, for example, that the images may be intercepted by hackers en route, 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 and the size of the internal network increase and are especially high if the video footage is broadcast to a multitude of recipients or posted on the internet.

2.5.5. Do the Guidelines also apply if the video-surveillance is carried out by an outsourced company?

The Regulation, and therefore, also the Guidelines, apply to the activities of the Community institutions and bodies.¹² However, even 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”.

¹² See Article 3(1) of the Regulation.

Example:

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

More guidance on outsourcing can be found in Section 14.1 below.

3 "Privacy by design"

3.1 Data protection as an integral part of project planning and implementation

When deciding whether to use video-surveillance technology (installing a new system or updating an existing system) and when planning and implementing such a system, data protection concerns must be considered as part of the project planning and implementation on an ongoing basis from the very early planning stage until the project will be completed. Throughout the project planning and implementation process, close cooperation with the DPO is strongly recommended to ensure that the system is no more intrusive than necessary and to establish an appropriate set of safeguards.

From a practical point of view it is important to carry out at least an initial data protection assessment with the assistance of the DPO before any financial commitments are made. This may prevent costly mistakes.

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 to operate the video-surveillance system. Before an internal decision is made to commission the system, a preliminary data protection analysis must be carried out with the assistance of your DPO. 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.

3.2 "Privacy and data protection impact assessment"

Whenever the risks to privacy and other fundamental rights so require (e.g. if a system is particularly complex, novel, or intrusive), a "privacy and data protection impact assessment" must be carried out before installing and implementing the

system.¹³ The purpose of the privacy and data protection impact assessment is to determine the impacts of the proposed system on the individuals' privacy and other fundamental rights and identify ways to mitigate or avoid any adverse effects.

Without prejudice to the generality of the foregoing, a privacy and data protection impact assessment should, in any event, be carried out in case of video-surveillance systems described in

- § Section 2.3 of these Guidelines (video-surveillance for purposes other than security, including video-surveillance proposed to be used for investigative purposes),
- § Sections 5.7 and 5.8 (employee monitoring and webcams),
- § Section 6.1 (camera locations beyond standard recommendations) and
- § Sections 6.5-6.12 (monitoring on Member State territory and in third countries; special categories of data; areas under heightened expectations of privacy; high-tech or intelligent video-surveillance; interconnected systems; covert surveillance; sound-recording and "talking CCTV").

A privacy and data protection impact assessment is also required if an Institution wishes to deviate its practices, to a significant degree, from the data protection safeguards proposed in these Guidelines.

In case of doubt whether a privacy and data protection impact assessment is necessary, please consult the EDPS.

The effort that is appropriate to invest in a privacy and data protection impact assessment depends on the circumstances. A project with large inherent risks warrants investment of much more effort than one with a comparatively limited impact on privacy and other fundamental rights. The privacy and data protection 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 privacy and data protection impact assessment an Institution may decide

- § to refrain from the planned monitoring or
- § to implement additional safeguards over and above those set forth in these Guidelines.

The impact assessment must be adequately documented in a privacy and data protection impact assessment report. The report must clearly specify the risks to

¹³ For systems which would have required such assessment but which are already in operation at the date of coming into force of these Guidelines, a privacy and data protection impact assessment must be carried out retroactively. See Section 15 for more detail on transitory provisions and how to ensure compliance for existing systems.

privacy and/or other fundamental rights that the Institution identified and the additional safeguards proposed.¹⁴

Example:

Your Institution considers the installation of body scanners at its entrances for the case of a perceived need for heightened security during special events or in case of a heightened state of security alert at the national level. This is 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 the prior checking procedure).

In case a privacy and data protection impact assessment is not required, the Institution should simply carry out a data protection compliance audit (or self-audit), as discussed in Sections 3.5 and 13 below. The purpose of this simpler exercise is to assess compliance with the provisions of the Guidelines and the Regulation. The audit will normally raise only few, if any, complex or novel issues not already addressed in the Guidelines.

3.3 Privacy-friendly technological solutions

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

Examples:

Encrypting data is helpful to reduce the potential damage in case of unauthorized access to the images.

Image scrambling can help eliminate surveillance of areas irrelevant to your surveillance target. This technique is also useful when you need to edit out images of third persons when providing access to his image to a data subject upon his request.

Watermarks can help ensure that the recordings are not tampered with.

¹⁴ The fact that a privacy and data protection impact assessment is required does not also always necessarily mean that you need to subject your plans to the EDPS for prior checking, although this will often be the case. For further information on prior checking, see Section 4.3 and Appendix 1.

3.4 Consultation of stakeholders and competent authorities

Consultation with stakeholders and competent authorities is essential in order to identify all relevant data protection concerns. Section 4 explains whom to consult when planning a new system. Recommendations include that in addition to the DPO of your Institution, you should also consult the staff committee in all cases when staff members may be caught on the cameras. In some cases, local authorities should also be contacted. Finally, in some cases the proposed system must also be submitted to the EDPS for prior checking.¹⁵

As these consultations may take time and may result in a need to change the system, these time frames must be kept in mind and the various consultations must be integrated into the project planning and implementing cycle.

3.5 Verification and documentation of compliance

Section 13 provides more guidance on how to maintain data protection compliance on an ongoing basis, and how to verify and document good administration. Recommendations in this Section include the adoption of a comprehensive video-surveillance policy and carrying out a self-audit (or third-party audit) measuring the data protection compliance of the video-surveillance system.

3.6 Timely planning for *ad hoc* surveillance operations

Finally, it must not be overlooked that video-surveillance may not only be about day-to-day CCTV operations. Advance plans must also be made if an Institution contemplates using video-surveillance in the future on an *ad hoc* basis (for example at times of hosting high-profile events or during eventual future internal investigations). In this case the necessary framework and policies for data protection must be established in time before the occurrence of such *ad hoc* need for video-surveillance.

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.*

In both cases your data protection assessment should include the additional video-surveillance activities that may be necessary at such times.

¹⁵ Regarding prior checking by the EDPS, please see Section 4.3 and Appendix 1.

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, depending on the circumstances of the case, some or all of the following individuals or organizations should be consulted:

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

4.1 Involvement and role of the DPO

The plans to install a video-surveillance system or to upgrade an existing one, as well as any other plans for video-surveillance that fall within the scope of these Guidelines, first and foremost, must be communicated to the DPO of the Institution. He or she must be consulted in all cases and must be involved through all stages of the decision-making process.

Examples:

The DPO should be participating in the initial determination whether to use video-surveillance technology, as discussed in Section 3.1. The DPO should be also called upon to provide expert advice on developing data-protection-friendly procedures. He or she should also be called upon to comment on the documents listed in Section 13 below (including all documents that form annexes to the Institution's video-surveillance policy, among others, the Institution's data protection notice on video-surveillance), 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 Consultation with the staff committee and other stakeholders

After initial consultation with the DPO of the Institution, staff representatives (including the staff committee) should also be consulted in all cases where staff may be captured on cameras. Consultation is required even if the purpose of the processing is not to monitor or evaluate the performance of staff members.

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 minimize 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 of 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 the cases described in Appendix 1 the DPO of the Institution must submit a prior checking notification to the EDPS.¹⁶ 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.

4.4 Involvement of National Data Protection Authorities

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. The provisions of the Regulation also apply.¹⁷ However, the data protection authority of the Member State in which the Institution is located may also have an interest and might arguably also claim to have concurrent jurisdiction with respect to monitoring that takes place

¹⁶ See Article 27 of the Regulation.

¹⁷ See Articles 3(1) and 41(2) of the Regulation.

outside the buildings. It may also wish to apply its own data protection laws.¹⁸ This parallel jurisdiction and applicability of national 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 and immunities of the European Communities (1965).¹⁹

The EDPS and data protection authorities in Member States will cooperate, should the need arise.²⁰

Section 6.5 provides a set of recommendations aiming at minimizing monitoring on Member State territory. These recommendations are set forth to encourage good data protection practice, but also, to avoid, or minimize, the duplication of efforts and the uncertainty that may arise from concurrent applicability of two data protection laws 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. Among others, as a matter of good practice, the final EDPS prior checking opinion, when applicable, may also be sent to the competent national 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 both (i) the potential benefits and (ii) the impact that the surveillance may have on the rights to privacy and other fundamental rights and legitimate interests of those in the area of coverage. Subsections 5.1-5.6 provide guidance on the main issues that need to be considered. Subsections 5.7-5.8 discuss some of the specific issues of employee monitoring and webcams.

This analysis 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

¹⁸ See Article 4 of Directive 95/46/EC (the "**Directive**").

¹⁹ 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.

²⁰ See Article 28(6) of the Directive and Article 46(f) of the Regulation.

level of impact it is likely to have on people's privacy and other legitimate interests or fundamental rights.

5.1 What are the benefits to be gained from the use of video-surveillance? Is the purpose of the system clearly specified, explicit and legitimate?

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.²¹

The designation of the purpose must be clear, specific and explicit and it must be put down in writing. Vague, ambiguous, or simply too general descriptions are not sufficient.

Example:

In most cases the purpose of video-surveillance is security-related. However, merely stating that the purpose is to "observe any anomalies inside the security perimeter", or "to deal with security incidents" is not sufficient without further detailing as to what will be considered as security incidents.

Instead, for example, you may wish to describe that the video-surveillance system helps control access to your buildings and helps ensure the security of your buildings, the safety of your 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 taken pursuant to your 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 your Institution, visitors or staff or threats to the safety of personnel working at the office (e.g. fire, physical assault).

These and similar security purposes should be clearly identified and outlined right from the outset. Where relevant, additional, specific security purposes should also be explicitly stated, such as protection against terrorist attacks, protection of visiting heads of States during international summits or protection of nuclear research facilities.

Institutions must also always communicate the purposes of the system to the public (i) on the spot at least in a summary form and (ii) via their on-line data protection notices.²²

²¹ See Regulation, Article 4(b).

²² See Section 11 for further guidance on how to provide notice to the public. For examples of the level of detail recommended for these communications, please see Appendices 3 and 4.

They must also clearly establish any significant limitations on the use of the data, especially if this is specifically requested by staff representatives or other stakeholders. The Institutions should, for example, specify that video-surveillance is not used to control the performance of the employee's work and will also not be used as an investigative tool or evidence in internal investigations or in disciplinary procedures, unless a security incident or criminal behaviour is involved.²³

It is also important to ensure that the data are not subsequently used for previously unforeseen purposes or disclosed to previously unforeseen recipients who might use it for additional, unrelated purposes ("**function creep**").

Example:

When the video-surveillance system is installed for security purposes and was announced as such to staff, recordings cannot be used to assess how well staff perform their job or whether they come to work on time.

5.2 Does the Institution have a lawful ground for the video-surveillance?²⁴

If an Institution carries out video-surveillance exclusively to control access to its buildings and to help ensure the security of its buildings, the safety of staff and visitors, as well as to protect property and information located on the premises, that is, if it uses video-surveillance for standard security and access control purposes, one may consider this as *potentially* necessary for the management and functioning of the Institution, and thus, the video-surveillance system will be based on a lawful ground, as required under the Regulation.²⁵

If this is not the case, the question arises whether there are any other possible lawful grounds for the video-surveillance. Other available grounds for lawfulness may include, for example, if there is a legal obligation to carry out video-surveillance or if the individuals concerned have each given their unambiguous consent.²⁶ These situations, however, will be rare.

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

Once it is established for what purpose a video-surveillance system will be used, and satisfied that there is a lawful ground to pursue video-surveillance for such a

²³ If this is not the case, you must state it clearly in your data protection notice.

²⁴ See Article 5 of the Regulation.

²⁵ See Article 5(a) and recital 27 of the Regulation.

²⁶ See Articles 5(b) and (d).

purpose, one should justify that camera use is indeed *necessary* for this purpose.²⁷

As regards systems installed for security and access control, one should not only identify any security risks that may 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 must be documented in writing identifying and assessing any existing risks.

Example:

You 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.

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

Systems should not be installed if they are not effective in achieving their purported purposes.

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 unauthorized 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 is considered adequate unless it is not feasible or significantly less effective than video-surveillance or would involve disproportionate costs.

²⁷ 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:

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.

As far as video-surveillance for security and access control is concerned, mere availability of the technology at a relatively low cost is not sufficient to justify the use of video-technology. Other solutions, such as controls by security personnel, alarm systems, access control systems, armouring and reinforcing gates and doors, better lighting and others should also be considered. Only when such solutions alone are demonstrated to be insufficient, can video-surveillance be used. 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.

5.6 Do the benefits gained from video-surveillance outweigh its detrimental effects?²⁸

Finally, even if the Institution concludes that there is a clear need to use video-surveillance and there are not any other less intrusive methods available, it should not use this technology if the detrimental effects of video-surveillance are not outweighed by the benefits of the video-surveillance.

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 at the communal kitchen and lunch room, to help prevent or detect who "help themselves" from 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 may become 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.

²⁸ 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.

5.7 Employee monitoring

Overly intrusive monitoring measures can cause employees unnecessary stress and can also erode trust within the organization. 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.

As explained in Section 2.3, to decide whether video-surveillance for non-security purposes is permissible, and whether such use requires additional safeguards not provided for in these Guidelines, a case-by-case analysis is necessary.

Therefore, any such proposed video-surveillance is subject to privacy and data protection impact assessment by the Institution as described in Section 3.2. 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) must also 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.

5.8 Webcams

Webcams or video-broadcasts that are used for promotion of recreational, tourist or similar facilities offered by the Institution (e.g. visitors centre, fitness centre, cafeteria, visitors' gallery in a meeting room) are also subject to an impact assessment under Section 3.2. Their use is generally discouraged although in exceptional cases they may be permissible based on the informed and individual consent of each user of the facility. Special attention must 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 clear and informed consent of each individual user. The users of the facility must have a genuine choice whether to use the part of the area covered by the cameras or wish to remain off-footage 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 on the spot. In this case using the specific sign-posted part of the facility may constitute implied consent.

6 Selecting, siting and configuring your 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 minimize any negative impact on the privacy and other fundamental rights and legitimate interests of those under surveillance.²⁹

6.1 Camera locations and viewing angles

Camera locations should be chosen to minimise viewing areas that are not relevant for the intended purposes.

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

Examples:

When a camera is installed on a rooftop to monitor an emergency fire exit, it must be ensured that the camera is not positioned 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, it must be ensured that the camera is not positioned to also incidentally record the entry to the neighbouring private office of a staff member.

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 authorized personnel to place 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 is possible that security requirements may warrant more extensive monitoring within the buildings. Should this be the case, such plans should specifically be discussed in the video-surveillance policy, including a justification for the need and proportionality of such additional camera locations. Any such proposed video-surveillance is subject to privacy and data protection impact assessment by the Institution as described in Section 3.2 above.

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 and the justification for the size of the system 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 whenever 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 opening from 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 recognizable 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 recognizable facial images are captured.

Example:

In some situations identifying individuals is not necessary and it is sufficient if 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 (or on the territory of third countries). 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 meters of the surrounding public space (providing mostly images of passers-bys in a busy street). This practice is permissible. However, it should be avoided that the cameras also monitor the windows of an apartment building opposite the protected building. The location or pointing of the cameras should be modified, the images should be scrambled, or other similar measures should be taken.

In all cases where monitoring goes beyond monitoring entry and exit points, a privacy and data protection impact assessment under Section 3.2 must be carried out. Such additional monitoring may only be carried out in case of demonstrated security needs and subject to additional safeguards, which may include, among others, the following:

- § limitation of monitoring adjacent *private* space (e.g. via scrambling images),
- § short retention periods not exceeding, as a rule, 48 hours (or live monitoring only),
- § limitation of the zooming capabilities of the cameras, or resolution of the cameras covering the surrounding public space, and
- § adequate training of the operators of the video-surveillance system to ensure that the privacy of passers-bys 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 stake-holders should also be considered.

In any case, it is important to bear in mind that the purpose of the video-surveillance, as a rule, cannot be general crime prevention or maintaining of law and order on Member State territory. These are the prerogatives of certain public authorities or organizations in Member States, subject to appropriate safeguards under national law. For example, local governments and/or local police may be the only ones authorized to operate such schemes. Therefore, in general, no Institution may legitimately use 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 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. Please refer to Section 4 for more information on the involvement of stakeholders and national (or regional) data protection authorities. Any such proposed video-surveillance is subject to privacy and data protection impact assessment by the Institution as described in Section 3.2.

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 required³⁰, 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 if such cooperation does not jeopardize their security.

Where a prior checking notification is required³¹, 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

The Institution's video-surveillance system 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.³²

³⁰ See Appendix 1.

³¹ See Appendix 1.

³² See Article 10 of the Regulation.

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 the intention is not to collect such special categories of data.³³

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.

A privacy and data protection impact assessment under Section 3.2 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),
- § 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.

³³ 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.

A privacy and data protection impact assessment under Section 3.2 must be carried out in case the Institution wishes to derogate from these rules. A prior checking by the EDPS will also be required.

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 a privacy and data protection impact assessment under Section 3.2. They are also subject to prior checking. The EDPS will assess, on a case by case basis, 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 other databases (e.g. a database of photos of suspected individuals for facial 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 multiple 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)
- § special purpose cameras with enhanced optical and digital zooming capabilities.

Use of cameras equipped with motion detection to limit video signals to events worthy of observation and recording, in itself, does not require a privacy and data protection impact assessment or prior checking. Neither is a privacy and data protection impact assessment or prior checking required merely because the motion detection system is configured 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). Cameras with customary panning, tilting and limited optical and digital zooming capabilities, for these reasons alone, are also not subject to a privacy and data protection impact assessment.

In case of doubt whether privacy and data protection impact assessment or 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 a privacy and data protection impact assessment under Section 3.2. A privacy and data protection 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 conspicuous 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 such areas (e.g. individual offices) in a more detailed data protection notice 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, a privacy and data protection impact assessment under Section 3.2 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 in a formal, legally required or authorized, investigation by Member State police, other competent law enforcement agents or by competent EU investigatory bodies a sufficiently serious criminal offence;
- § the use of covert surveillance is in accordance with the law and has been formally authorized 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”³⁴

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 must 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, a privacy and data protection impact assessment under Section 3.2 and must undergo prior checking.

7 How long can the recordings be kept?

7.1 Retention period

Recordings should not be retained longer than necessary for the specific purposes for which they were made.³⁵ It should also be considered whether recording is necessary in the first place and whether live monitoring without recording would not 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 support on a first-in, first-out basis. Once the media support is no longer useable (after many cycles of use) it

³⁴ 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”).

³⁵ Regulation, Article 4(1)(e).

should 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, 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 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.

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.³⁶ In most cases a shorter period should suffice.

In case the surveillance covers any area outside the buildings on Member State territory (typically those near entrance and exit areas) and it is not possible to avoid that passers-by or passing cars will be inadvertently caught on the cameras, the maximum recommended period of retention is 48 hours.

³⁶ 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.

Please note also that when a prior checking is required, or if it is otherwise necessary to provide adequate safeguards due to the intrusiveness of the processing operation or the specific circumstances of the case, the EDPS may impose shorter retention periods to minimize the intrusion to 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 (or consider live monitoring only).

7.2 Register of recordings retained beyond the retention period

A register must be held to keep track of any recording that is retained beyond the normal retention period, indicating (i) the date and time of the footage and camera location, (ii) a short description of the security incident, (iii) the reason why the footage needs to be retained and (iv) the expected date of the review of the necessity to retain the footage any further.

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 authorized users can access only those personal data to which their access rights refer.³⁷ 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 any access rights of any persons. Any grant, alteration or annulment of access rights must be made pursuant to criteria established in the Institution's video-surveillance policy.

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

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

³⁷ See, in this latter respect, Regulation, Article 22.2(e)

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, 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 password of one individual may allow copying recorded footage, while the password 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 password allows copying or deletion, is actually authorized 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 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, must be given data protection training and must be familiar with the provisions of these Guidelines inasmuch as these are relevant to their tasks. The training must pay special attention to the need to prevent the disclosure of video-surveillance footage to anyone other than authorized individuals.

Trainings should be held when a new system is installed, when significant modifications are made in the system, when a new person takes up his/her duties, as well as periodically afterwards at regular intervals. For existing systems, a first training should be held within six months as of the date of coming into force of these Guidelines.

8.3 Confidentiality undertakings

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, must sign confidentiality undertakings to ensure that they will not transfer, show, or otherwise disclose the content of any video-surveillance footage to anyone who has no right of access (this usually means anyone outside the Institution's security unit).

9 What security measures should be taken to protect the data?

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.

When determining the necessary security measures,

- § in addition to taking into account the provisions of the Regulation³⁸,
- § the Institution should also carefully consider the EDPS recommendations made in his "Security Guidelines for data controllers with regard to the processing of personal data" (available on the EDPS website at www.edps.europa.eu)³⁹, which are applicable with respect to all data processing operations by the Institutions,
- § as well as the recommendations set forth in this document specifically for video-surveillance.

Appropriate measures must be taken to ensure security with respect to (i) transmission, (ii) storage (such as in computer databases), and (iii) access (such as access to computer systems and premises).

Transmission must be routed through secure communication channels, 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 appropriately secured. Physical access to the control room and the room storing the video-surveillance footage should be protected. No third parties (e.g. cleaning personnel, constructors or repairmen, or any other employees other than security staff) should have unsupervised access to these premises.

The location of monitors should be chosen so that unauthorized personnel cannot view them. If they must be near the reception area, the monitors must be positioned so that only the security personnel could view them and not people exiting or entering the building.

A reliable digital logging system must be in place to ensure that a security audit can determine at any time who accessed the system, where and when. The logging system should be able to identify who viewed, deleted, copied or altered any video-surveillance footage. In this respect, and elsewhere, particular attention should 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

³⁸ See Article 22 of the Regulation.

³⁹ PM: At the time of circulating this consultation draft of the Video-surveillance Guidelines, the EDPS Security Guidelines are under preparation and not yet publicly available.

disclosure of personal information. This should include, whenever possible, notification of the breach to those whose data are inadvertently disclosed.

The security analysis as well as the measures taken to protect the video-surveillance footage should be adequately documented and should 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 in-house and outside the Institution

10.1 General framework for transfers

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.⁴⁰

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 your tasks to be carried out⁴¹ 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 should be made for purposes that are incompatible with the initially specified purpose for the video-surveillance system.

⁴⁰ 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).

⁴¹ 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 local police in connection with criminal investigations.

Example:

When 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 only few, although potentially important exceptions to this rule.⁴² The most relevant of these exceptions is when the transfer is requested by national police for the investigation or prosecution of criminal offences. This is discussed in Section 10.4 below.

10.2 The role of the DPO: *ad hoc* and systematic or repeat transfers

Whether a transfer can be made often requires a very delicate balancing exercise between the rights of the individual who was captured on the recordings and the rights or interests of those requesting the footage. Every transfer must be carefully assessed on its own merits, on a case by case basis.

The DPO should be able to help assess whether the transfer is lawful under the Regulation and his/her advice should always be sought when in doubt. He or she should be consulted in case of each *ad hoc* transfer.

However, if similar transfers are carried out repeatedly, the data protection assessment may also be similar. If this is the case, these transfers should be described in your Institution's video-surveillance policy referred to in Section 13.1. They must also be mentioned in the notice to the public under Section 11. Once a policy regarding transfers is in place, there is no need to specifically consult your 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. There will be no need to consult your DPO each time.

⁴² See Article 20 of the Regulation.

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 some 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.

Please note that such transfers are exceptional. The purpose of a system installed for security purposes, as noted in Section 2.2 above, is to help prevent, deter and investigate security incidents (e.g. fire, break-in or other unauthorized access).

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 to check data protection compliance of an Institution’s video-surveillance practices or when the EDPS is investigating a complaint against any particular person involved.

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 a 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 organization 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 must 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 with the participation of illegal immigrants to highlight the issue of the need of regularization of their situation. At the end of what turned out to be a peaceful demonstration with no security incidents, the national police requests you to 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 when such need arises. You should not accommodate such a request.

Please note also that if a Member State police or other national organization 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 Institution must keep a register of transfers and disclosures. In it, each instance must be registered when a transfer has been made to third parties. (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 at least include (i) the date of the recordings, (ii) the requesting party (name, title and organization), (iii) the name and title of the person authorizing the transfer, (iv) a brief description of the content of the recordings, (v) the reason for the request and the reason for granting it, and finally, (vi) 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 at any time to submit a copy of the register for inspection and answer any related questions.

11 How to provide information to the public

Information must be provided to the public about the video-surveillance in an effective and comprehensive manner.⁴³

To this end, these Guidelines recommend a multi-layer approach, which consists of a combination of at least the following two primary 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 an intranet and also on the internet for those who wish to know more about the video-surveillance practices of the Institution.

These two recommended methods can be complemented by others. For example, printed hard-copies or print-outs of the same 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 internet (and on leaflets and via other means) must not altogether substitute the on-the-spot notices. Rather, they should serve as a complement to them.

The on-the-spot notices should include a pictogram (e.g. the ISO pictogram or the pictogram customarily used in the area or country where the building is located) and as much of the information listed under Article 12 of the Regulation as is reasonable under the circumstances. In any event, they must at least identify the "controller" (in this context the name of the Institution is usually sufficient) and the purpose of the surveillance ("for your safety and security" is usually sufficient). They must also clearly mention that the images are not only viewed but are also recorded, provide contact information and mention the availability of further information (a link to the internet address of the data protection notice should always be included). If any area outside buildings is under surveillance, this should be clearly stated. A notice in such case merely stating that "*the building* is subject to video-surveillance" is misleading.

All members of the security staff and reception should be trained on the privacy aspects of video-surveillance practices and should be able to make copies of the detailed privacy policies instantly available upon request. They should also be able to tell members of the public whom to contact if they have additional questions or would like to request access to their data.

⁴³ For the list of items required by law to be included in your notice, see Article 12 of the Regulation.

The signs must be placed at such locations and in such size 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 persons, is located in a four-storey building in a densely built-up urban area with some pedestrian traffic on the street outside the main entrance. 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 should 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) should 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 or at the entrance to the cafeteria).⁴⁴

A sample on-the-spot notice is given in Appendix 3. However, there is no need to follow the format of the sample strictly. Many improvements and variations on this sample notice are possible. In addition, the customary signage in the Member State where the building is located may also be taken into account.

As for the more detailed on-line data protection notice on video-surveillance, this document must include at least the following information in a 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 must also be clearly specified, see Section 5.1),
- § who has access to the video-surveillance footage, and to whom the images may be disclosed,
- § how the information is protected and safeguarded,

⁴⁴ See also Section 6.11 on covert video-surveillance.

- § 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 have recourse at any time to the EDPS.

Finally, the notice should also point out the fact that the video-surveillance system is set up in compliance with the recommendations set forth in the Guidelines and provide a link to the internet address where the Guidelines are available (e.g. to the relevant part of the EDPS website). A link to the video-surveillance policy and to the data protection compliance report/s should also be provided. If a privacy and data protection impact assessment has been carried out, this should be referenced in the notice and a link to the report must also be provided. Finally, if the system has been prior-checked by the EDPS, this should be specifically mentioned, and a link should be provided to the EDPS prior checking Opinion.

To illustrate the level of detail that the EDPS recommends, Appendix 4 provides a sample on-line data protection notice for a relatively simple standard video-surveillance system. Of course, in each case, there may be differences, considering the circumstances of the case.

In addition to the generic notice described above, individuals must also be given specific individual notice

- § if they were identified on camera by security staff in a security investigation provided that
- § (i) their identity is noted in the files, (ii) the recording is used against them, (iii) kept following the regular retention period, (iv) transferred outside the security unit *or* (v) 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.⁴⁵ If such a situation arises, please seek advice from the DPO.

12 How to fulfil access requests by members of the public

When asked by an individual what data the video-surveillance system processes about him/her, this request must be answered in a timely manner and in as much detail as it is reasonable under the circumstances to accommodate his/her concerns.

If the request is very general, it is usually sufficient to refer the individual to the text of the data protection notice posted on the Institution's website and/or provide a copy of it.

⁴⁵ Other exceptions under Article 20 of the Regulation may apply in exceptional circumstances.

Example:

A citizen 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 data protection notice 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 scrambling). Protection of the rights of third parties, however, should not be used as an excuse to prevent legitimate claims of access of individuals against whom the 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 was it 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 must also be a default policy for the provision of 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 data protection notice and 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) cannot be delayed beyond the three months maximum period provided for in the Regulation⁴⁶. In most cases, the access should be granted much earlier.

If the request is urgent, the request should 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. For the case of disagreement between the Institution and the individual requesting access, a simple and efficient internal review or complaint procedure must be put in place. This should be available not only to staff members, but also to third parties who request access to their rights.

The public must be informed about the review procedure both in the detailed data protection notice and in the response to the access request.

13 Maintaining, verifying and documenting good administration

To ensure transparency and good administration, and to provide evidence of compliance, each Institution should verify and document the compliance of its practices with the provisions of these Guidelines. In particular, each Institution should

⁴⁶ See Article 13 of the Regulation.

- § adopt a video-surveillance policy, and
- § carry out a self-audit or third party audit and document its results in an audit-report (“**data protection compliance report**”).

In addition, in the cases referred to in Section 3.2, a privacy and data protection impact assessment must also be carried out and documented in a privacy and data protection impact assessment report.

Appendix 2 provides a simple template for a video-surveillance policy that may be appropriate for a small agency using a simple video-surveillance system. If the Institution uses video-surveillance more extensively, or its practices differ from the standards recommended in the Guidelines, the policy should be more detailed and more extensive. This is also true for the data protection compliance report.

13.1 Video-surveillance policy

This document should

- § give an overview of the video-surveillance system and describe its purposes,
- § confirm compliance with the Regulation and the Guidelines,
- § describe any differences from, or additions to, the standard practices recommended in the Guidelines and explain the reasons therefore, and
- § outline any necessary implementing measures.

The video-surveillance policy has to be made publicly available. If any part of this document contains confidential information, both a confidential and a non-confidential version must be prepared and the non-confidential version must be made publicly available. For example, if necessary, the public version of the part on security measures may be drafted in a summary fashion to ensure that the security of the system is not jeopardized.

13.2 Data protection compliance report

The Institution should verify and document the compliance of its practices with the provisions of the Regulation and these Guidelines. This exercise 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. In either case, the audit must address certain key items of compliance and the results of it should be summarized in a written data protection compliance report.

This exercise must be done prior to the launch of the video-surveillance system but also periodically afterwards. The periodic self-assessment should take place at least once every 2 years and also every time when a significant change in the circumstances warrants a review. Installation of additional cameras or other system upgrades should normally warrant a review.

14 Outsourcing and video-surveillance by other third parties

14.1 Outsourcing video-surveillance

If the Institution decides to outsource any part of its video-surveillance operations, it will remain liable as a "controller". Due diligence should be used in choosing the contractors and a proactive approach should be taken in 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, if any.

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 should also clearly and specifically refer to the contracted company's obligations regarding (i) security, (ii) confidentiality, and (iii) its obligation to act only upon your Institution's instructions.⁴⁷ The contracted company must also provide appropriate training to its staff, including training on data protection and the provisions of the Guidelines relevant to their work.

With regard to subcontracting, it must be made sure that any direct or indirect subcontractor will be bound by the same obligations as the direct contractor. It should be possible 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 that appropriate data protection notice should be given to the public, including the Institution's staff.

14.2 Video-surveillance by other third parties

This Section applies to the Institution if it neither carries out the video-surveillance itself, nor has outsourced this task to a third party. This may be the case, in particular, where the video-surveillance is carried out by a landlord or by an contracted company on behalf of the landlord. In some cases there may be a complex contractual system involving several leases and subleases, and/or several

⁴⁷ For more details, see Articles 22 and 23 of the Regulation.

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 out-sources maintenance of the building to company D. Company D, in turn, out-sources 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 cases in such situations the Institution will not be technically considered as 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. it should negotiate that the controller puts up appropriate on-the-spot notices and provides more detailed information that can be posted on the Institution's website).

15 Transitory provisions and future updates

These 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 has six months as of the date of publication, that is, until **[1 May 2010]** to bring its existing practices in line with the recommendations contained in the Guidelines.

Ex-post review of compliance status and ex-post prior checking⁴⁸

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

- § confirming that the Institution adopted a video-surveillance policy (see Section 13.1) and
- § carried out a self-audit or third-party audit (see Section 13.2);
- § specifying whether the Institution also carried out a privacy and data protection impact assessment (Section 3.2) with respect to any particular issue/s; and
- § informing the EDPS whether based on the findings of the data protection compliance report, and the privacy and data protection impact assessment, the Institution believes that an ex-post prior checking is necessary with respect to any particular issue/s.

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.

A copy of the video-surveillance policy (along with its attachments) as well as a copy of the data protection compliance report and the privacy and data protection impact assessment report should be attached to the letter. There is no need to send any additional information or a prior checking notification form to the EDPS. Early compliance and notification on compliance status prior to the final deadline are welcome and encouraged.

For further information regarding the procedure, please refer to Appendix 1. If in doubt, please consult the EDPS who will provide additional guidance as necessary. The EDPS is also available for consultation on any other issues that may arise during the transition period.

After the lapse of the six month deadline, 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. If necessary, the procedure may also include on-the-spot 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.

Pending ex-post prior checking notifications

Due to the changes that will be required by the Institutions to bring their practices in line with the recommendations set forth in the Guidelines, the EDPS intends to close all ex-post prior checking notifications which were submitted prior to the coming into force 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 six months deadline regarding their compliance status.

Prior checking notifications and/or compliance update for new systems

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

Revision of the Guidelines

When significant changes in the circumstances so require, the EDPS will consider issuing revised versions of these Guidelines. The circumstances which may trigger

such 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
- § Comments received

Appendix 1: Further information on prior checking by the EDPS

1.1. What is prior checking?

Article 27 of the Regulation provides 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".

1.2. Does video-surveillance pose “specific risks”?

Video-surveillance, by its nature, has a strong capacity of being privacy invasive. In addition, wide-spread video-surveillance also has significant social costs and - beyond privacy - may also negatively affect the exercise of several other fundamental rights.

Due to these considerations, the EDPS concluded that video-surveillance is in many situations likely to present specific risks to the rights and freedoms of data subjects, in the meaning of Article 27(1), and therefore, it is in principle subject to prior checking.

Some video-surveillance practices may also fall under one of the “specific risk” categories listed under Article 27(2). For example, some employee monitoring may involve performance evaluation, and thus, may require prior checking also under Article 27(2)(b). Video-surveillance for investigatory purposes is likely to concern data related to suspected offences, and thus, may also require prior checking under Article 27(2)(a).

1.3. Does this mean that the EDPS needs to review in detail and prior check each video-surveillance system individually?

No, this does not mean that the EDPS needs to review comprehensively and in detail every single video-surveillance system operated by or on behalf of every Institution.

The Guidelines set forth a comprehensive set of data protection guidelines for relatively simple static video-surveillance systems established for common security purposes. To address and minimize the “specific risks” of video-surveillance, for these standard systems it is often sufficient if such a video-surveillance system is

- § designed after careful consideration of its data protection impacts and
- § adoption of a comprehensive set of standard data protection safeguards as recommended in the Guidelines, and
- § the Institution verifies and self-certifies compliance with the Regulation and the Guidelines, and notifies the EDPS of its compliance status (see Section 13).

Some video-surveillance systems, however, remain subject to prior-checking. The purpose of this more in-depth review in the framework of a prior checking procedure

is to provide the Institutions with additional and tailor-made recommendations beyond those already set forth in these Guidelines. If a prior checking notification is required, the comments and recommendations of the EDPS will be set forth in a formal Opinion.

The following remain subject to prior-checking:

- § video-surveillance proposed for investigative purposes (Section 2.2, second example)
- § video-surveillance for purposes of monitoring employees (Section 5.7),
- § video-surveillance processing special categories of data (Section 6.7);
- § monitoring in areas under heightened expectation 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).

In addition, it is possible that some types of video-surveillance not already mentioned above might fall under Article 27(2)(a) through (d).

In case of doubt whether a prior checking is necessary, please consult the EDPS.

1.4. When there is a prior checking and more in-depth review by the EDPS, will it be comprehensive and cover all aspects of a video-surveillance system?

No, in most cases a prior checking and more in-depth review does not also mean that the EDPS will comprehensively review and comment on all aspects of the Institution's video-surveillance practices. Instead, the EDPS will usually focus only on those aspects of video-surveillance which differ from, or are in addition to, the common practices and standard safeguards set forth in the Guidelines.

Example: You plan to equip some cameras with a sound-recording feature. In all other aspects, you comply with the recommendations of the Guidelines. As a general rule, the EDPS will only focus on this single issue in his Opinion.

However, in some cases, the EDPS may, at his own initiative, nevertheless carry out a more comprehensive review. This may be the case, for example,

- § if it is difficult to assess individual aspects of the video-surveillance system without the entirety of the system, especially if the system is complex or if a large number of exceptions, or very significant exceptions are proposed from the standard practices and recommendations set forth in the Guidelines,
- § if reasonable doubts arose regarding compliance of the remaining aspects of the system despite self-certification of compliance or
- § if the quality of the notification is poor and it is impossible or difficult to ascertain compliance without a more comprehensive review.

1.5. Do we always need to notify the EDPS about our compliance status when we install a new video-surveillance system?

Yes, whether or not a prior-checking and an in-depth review of your system will be necessary, your DPO must always notify the EDPS regarding your compliance status. Your video-surveillance policy (along with its attachments) as well as a copy of your data protection compliance report, and your privacy and data protection impact assessment report, if applicable, should always be attached to this letter. There is no need to send any additional prior checking notification form to the EDPS.

1.6. When do we need to submit a prior checking notification to the EDPS and how long does it take for the EDPS to issue his Opinion?

The EDPS has two months to issue his prior checking opinion, which, in case the complexity of the case so requires, may be extended by an additional two months. These timelines are suspended if the EDPS requests further information that you need to provide.⁴⁹

You cannot start using the new video-surveillance system before the EDPS has issued his Opinion and you followed-up and addressed his concerns.⁵⁰

Considering these timelines, you should aim at submitting your prior checking notification to the EDPS well in time *before you wish to start operating the new system*. However, whenever possible, it is advisable to send your notification even earlier, well in time *before you make any financial commitments to your new system*. This is especially recommended if doubts arose regarding the data protection aspects of your planned system during the initial assessment and consultation process or if your system is particularly complex. Such an early notification may ensure that you do not incur financial losses in case the EDPS requires major changes in your system (for example, if he concludes that some cameras should not be used at all or their specifications or locations need to be changed).

Based on the foregoing, the EDPS recommends that you allow at least four months for the EDPS to process your notification before the proposed launch date. More, if you expect lengthy exchanges, meetings, and on-the-spot checks in the framework of prior checking a complex or controversial proposal.

1.6. When do we need to notify the EDPS regarding our compliance status in cases where no prior checking is required?

⁴⁹ See Regulation, Article 27(4).

⁵⁰ This is apart from the case of ex-post prior checking. Please also note that if you wish to conduct a pilot to test the system for a limited period of time and with limited coverage, the EDPS may be able to issue a provisional authorization for you for the duration of the pilot, subject to adequate provisional safeguards. Please check the modalities of this with your DPO.

If you are confident that your system is in full compliance with the Regulation and the Guidelines, have verified this, and can confidently self-certify that this is the case (in agreement with your DPO), then it is sufficient if you send a confirmation of your compliance status to the EDPS before you wish to launch your system.

1.7. What else do I need to do during the prior checking procedure?

Once you submitted your notification via your DPO, you should also (i) be available to submit any additional information in a timely manner that may be requested by the EDPS during the prior checking procedure, (ii) be ready for a meeting or an eventual on-the-spot inspection if necessary and (iii) be available to comment on the final draft of the Opinion.

1.8. Will the Opinion of the EDPS be made public?

The EDPS prior checking Opinion, after you will have had an opportunity to comment on it, will be published on the EDPS website. Certain confidential data, including the security measures you took to safeguard your video-surveillance system may be omitted from the published version of the Opinion.

Appendix 2: Sample video-surveillance policy for a small video-surveillance system

[Insert name of the Agency] Video-surveillance Policy

Adopted by the Director's Decision on [15 January 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 annexes, 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 what is our compliance status with applicable data protection laws?

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 _____ 2009. Our procedures, however, have since then been revised to comply with the recommendations set forth in the Guidelines (Guidelines, Section 15). **[Please provide a hyperlink to a copy of 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. **[Note that in case you deviate from any recommendations in the Guidelines, this must be clearly stated and justified in your video-surveillance policy, data protection compliance report and on-line data protection notice. In case of a significant deviation, you must also discuss this in your privacy and data protection impact assessment report.]**

2.3. Self-audit. The system was subject to a self-audit. **The Data Protection Compliance Report** is attached as **Annex 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 privacy and data protection impact assessment (Guidelines, Section 3.2) or to submit a prior checking notification to the EDPS (Guidelines, Section 4.3). **[Note that in case a privacy and data protection impact assessment is needed, your privacy and data protection impact assessment report must also be annexed 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 must also be annexed,**

and the main EDPS recommendations and your follow-up on those recommendations must be summarized in the policy itself.]

Simultaneously with adopting this Video-surveillance Policy, we also notify the EDPS of our compliance status by sending him a copy of our Video-surveillance Policy and our Data Protection Compliance Report.

2.5. Contacts with the national data protection authority. The national data protection authority in **[insert country]** was also already informed and its concerns and recommendations were taken into account. In particular, now both the on-the-spot notice and the more detailed data protection notice on the internet are also available in **[insert 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 on **[15 January 2010]** 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 the need for a video-surveillance system as proposed in this policy. We also 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 above in Section 1 (see Guidelines, Section 5). The concerns of the DPO and the Staff Committee were addressed (see Guidelines, Section 4).

2.7 Transparency. The Video-surveillance Policy has two versions, a version for restricted use and a public version available and posted on our internet and intranet sites at **[insert internet and intranet addresses]**. The public version of the Video-surveillance Policy may contain summary information with respect to particular topics or annexes. 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, for the first time by 15 January 2012. During the periodic reviews we will re-assess that:

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

The periodic reviews will also cover all other compliance issues addressed in the first Compliance Report. Copies of the **Periodic Data Protection Compliance Reports** will also be annexed to this Video-surveillance Policy in **Annex 1**.

2.9. Privacy-friendly technological solutions. In addition to a number of data protection safeguards, during the process of the current first revision of our video-surveillance practices, we also implemented the following privacy-friendly technological solutions (see Guidelines, Section 3.3):

[Please list and describe the solutions implemented.]

3. What areas are under surveillance?

The video-surveillance system consists of a set of seven fixed cameras. **A map with the locations of the cameras** is included in **Annex 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 minimize viewing 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 **Annex 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 taken pursuant to 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 or threats to the safety of 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. The system is also not used as an investigative tool or to obtain evidence in internal investigations or in disciplinary procedures, unless a security incident is involved. (In exceptional circumstances 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 2.2, 2.3 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 3.6). We also have no webcams (see Section 5.8 of the Guidelines).

4.5. 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?

We consider that the use of our video-surveillance system is necessary for the management and functioning of our Agency (namely 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).

The legal basis for the video-surveillance is 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 **Annex 4**.

6.2. Access rights. The Agency's Security Policy for Video-surveillance (see Section 7 below and Annex 7 hereto) 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 **[10 January 2009]**. There are trainings foreseen for each newcomer, as well as periodic workshops on data protection compliance issues 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 the participants each also signed a confidentiality undertaking. This undertaking was also signed by the outsourced company. Copies of these **confidentiality undertakings** are attached as **Annex 5** (see Section 8.3 of the Guidelines).

6.5. Transfers. All transfers 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 **Annex 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. Please also include them in your data protection notice.]**

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 was 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, and subject to the procedural safeguards noted above, access may also be given to

- § the European Anti-fraud Office (“**OLAF**”) in the framework of an investigation carried out by OLAF, or
- § 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

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.

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 set forth in a processing-specific security policy (“**Security Policy for Video-surveillance**”), which is attached as **Annex 7**.

The Agency's Security Policy for Video-surveillance was established in accordance with Section 9 of the EDPS Video-surveillance Guidelines and in accordance with the EDPS Security Guidelines for data controllers with regard to the processing of personal data (see www.edps.europa.eu).

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 right 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 grant, alteration or annulment of access rights is made pursuant to the criteria established in the Security Policy for Video-surveillance (see Annex 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 recorded 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 **Annex 6** (see Section 7 of the Guidelines.)

The system is also monitored live by the security guard at 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 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 your intranet and also on the internet for those who wish to know more about the video-surveillance practices of our Institution.

Print-outs of the same data protection notice are also available at our building reception and from our security unit upon request and a phone number and an email address is provided in the data protection notice for further enquiries.

We also provide notice on the spot next 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 **Annex 8**. Our on-line data protection notice is included as **Annex 9**.

9.2. Specific individual notice. In addition to the generic notice described above, individuals must also be given specific individual notice

- § if they were identified on camera by security staff in a security investigation provided that
- § (i) their identity is noted in the files, (ii) the recording is used against them, (iii) kept following the regular retention period (iv) transferred outside the security unit *or* (v) 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.⁵¹ If you face such a situation, please seek advice from your DPO.

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 regarding them and to correct and complete them. Any request for access, rectification, blocking and/or erasing of personal data should be directed to Ms/Mr _____, Head of Unit __ **[insert 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 must respond to an enquiry in substance within 15 calendar days. If this is not possible, the applicant must be 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 customary support. In case of such a request, the applicants must indicate their identity beyond doubt (e.g. they may bring identity cards when present themselves for the viewing) and also designate the date, time, location and circumstances when they were caught on cameras. They must also provide a recent photograph 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 apply in a specific case. For example, upon 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 to have 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

§ the head of the security unit (see contact details above), and/or

⁵¹ Other exceptions under Article 20 of the Regulation may also apply in exceptional circumstances.

- § 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.

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

* * *

Annexes to the Video-surveillance Policy:

- § **The Data Protection Compliance Report** is attached as **Annex 1**. Annex 1 also contains the **periodic reviews**.
- § A map with the locations of the cameras is included in **Annex 2**.
- § The **technical specifications** for the cameras and for the video-surveillance system as a whole (including any software and hardware) are included in **Annex 3**.
- § The **contract with the outsourced security company** is included in Annex 4.
- § Copies of the **confidentiality undertakings** are attached as **Annex 5** (see Section 8.3 of the Guidelines).
- § **The register of retention and transfers** is included in **Annex 6** (see Section 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 set forth in a processing-specific security policy ("**Security Policy for Video-surveillance**"), which is attached as **Annex 7**.
- § The Agency's **on-the-spot data protection notice** is included as **Annex 8**.
- § Our **on-line data protection notice** is included as **Annex 9**.

Appendix 3: Sample on-the-spot data protection notice

[Insert your video-surveillance logo: you may consider, for example, the ISO pictogram or the pictogram customarily used in the area or country where the building is 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.]**

[Insert name of your Institution] processes your images in accordance with

- § Regulation (EC) No 45/2001 on the protection of personal data by the Community institutions and bodies,
- § the Video-Surveillance Guidelines issued by the European Data Protection Supervisor, and
- § the Video-surveillance Policy of **[Insert name of your Institution]**.

For further information

- § please consult www.domainnameofyourinstitution/cctv or
- § contact: **[insert telephone number and email address for your security unit]**.

[Include multiple language versions if applicable.]

Appendix 4: Sample on-line data protection notice

Data protection notice for [the Agency's] video-surveillance system

For your safety and security, the security unit of our Agency operates a video-surveillance system. This notice

- § provides you with basic information about the system,
- § tells you where you can get more detailed information and
- § explains how you can exercise your rights as a data subject.

1. What areas are under surveillance?

The video-surveillance system consists of a set of seven fixed cameras. Of these, six cameras 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. For example, there are no cameras located in individual offices or in the hallways or lobby areas.

2. 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. The legal basis for the video-surveillance is the Agency's Video-surveillance Policy, which can be found at **[insert website address]**. This policy, in turn, forms part of the broader security policies adopted by our Agency.

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

The video-surveillance system is a conventional static system equipped with motion detection. It records any movement detected by the cameras in the area under surveillance, together with time, date and location. The image quality in most cases allows your identification if you are in the camera's area of coverage. The cameras are fixed, and thus, cannot be used by the operators to zoom in on you or follow you around.

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 taken pursuant to 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 or threats to the safety of personnel working at the office

(e.g. fire, physical assault).

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. The system is also not used as an investigative tool or to obtain evidence, unless a security incident is involved. (In exceptional circumstances the images may be transferred to investigatory bodies in the framework of a formal disciplinary or criminal investigation as described in Section 4 below.)

4. Who has access to your information and to whom is it disclosed?

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.

All transfers 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. 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. Please also include them in your data protection notice.]**

No access is given to management or human resources. **[If this is not the case, 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 this is needed to investigate or prosecute criminal offences. There were occasions in the past where police was given access to footage to help investigate bicycle theft from the bicycle racks located at the entrance to the garage.

Under exceptional circumstances, and subject to the procedural safeguards noted above, access may also be given to

- § the European Anti-fraud Office (“**OLAF**”) in the framework of an investigation carried out by OLAF, or
- § 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

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.

5. How do we protect and safeguard your information?

In order to protect your personal data, a number of technical and organisational measures have been put in place. 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 right 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 grant, alteration or annulment of access rights is made pursuant to criteria established in our security policy for video-surveillance, which forms an integral part of our video-surveillance policy.

6. How long do we keep your data?

The images are recorded 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.

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

7. How can you verify, modify or delete your information?

You have the right to access the personal data we hold regarding you and to correct and complete them. Any request for access, rectification, blocking and/or erasing your personal data should be directed to Ms/Mr _____, Head of Unit __ **[insert email address and telephone number]**. You may also contact him/her in case of any questions relating to the processing of your personal data.

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

If you specifically request, a viewing of your images may be arranged or you may obtain a copy of your recorded images on a DVD or other customary support. In case of such a request, please indicate your identity beyond doubt (e.g. you may bring your identity card when present yourself for the viewing) and also designate the date, time, location and circumstances when you were caught on cameras. Please also provide a recent photograph that allows the security staff to identify you from the images reviewed.

At this time, we do not charge you for requesting a viewing or a copy of your recorded images. However, we reserve the right to charge a reasonable amount in

case the number of such access requests increases.

Please also note that we cannot always provide you with an image as exemptions under Article 20(1) of Regulation 45/2001 may apply. For example, upon a case-by-case evaluation we may have to conclude that restricting your 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.

8. What is our compliance status with applicable data protection laws?

The Agency processes your images in accordance with the Video-Surveillance Guidelines issued by the European Data Protection Supervisor and Regulation (EC) No 45/2001 on the protection of personal data by the Community institutions and bodies. **[Note that in case you deviate from any recommendations in the Guidelines, this must be clearly stated in your on-line data protection notice.]** The system was subject to a self-audit. Considering the limited scope of the system, it was not necessary to submit a prior checking notification to the EDPS but we notified him of our compliance status by sending him a copy of our video-surveillance policy and data protection compliance report. The national data protection authority in **[insert country]** was also informed and its concerns and recommendations were also taken into account. A periodic data protection review is undertaken by the security unit every two years.

[Provide a hyperlink to

- § **the internet address where the Guidelines are available (e.g. to the relevant part of the EDPS website),**
- § **to your video-surveillance policy,**
- § **to your data protection compliance report/s, as well as**
- § **to your privacy and data protection impact report and**
- § **the EDPS prior checking Opinion where applicable.]**

9. Right of recourse

You have the right to have recourse to the European Data Protection Supervisor (edps@edps.europa.eu) if you consider that your rights under Regulation 45/2001 have been infringed as a result of the processing of your personal data by the Agency. Before you do so, we recommend that you first try to obtain recourse by contacting

- § 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]**

If you are a staff member you may also request a review from your appointing authority under Article 90 of the Staff Regulation.

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