EUROPEAN COMMISSION
DIRECTORATE-GENERAL
HUMAN RESOURCES AND SECURITY
Directorate HR.DS - Security
The Director

Brussels, July 2019
HR.DS/BA

EUROPEAN COMMISSION VIDEO SURVEILLANCE POLICY MANAGED BY THE SECURITY DIRECTORATE (HR.DS) (BRUSSELS AND LUXEMBOURG SITES)

1. Objective and scope of the video surveillance policy – exclusions

1.1. Introduction

The European Commission employs a video surveillance system at its sites in Brussels and Luxembourg to ensure the security of its buildings, property, staff and visitors. This video surveillance policy describes the video surveillance system at the above-mentioned sites and the safeguards adopted by the Security Directorate (HR.DS) to protect personal data, the right to privacy and the other fundamental rights and legitimate interests of individuals filmed by the system's cameras.

Unless explicitly stated in the Service Level Agreements (SLAs) made between the European Commission and the agencies in and around Brussels, this policy does not apply to the latter.

This policy comes under Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018[1] 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, repealing the Regulation n°45/2001, and to notification DPR-EC-00654.1 'Video surveillance – analogue and digital storage'.

1.2. Objective of the video surveillance system

The video surveillance system for which HR.DS is responsible is one of the resources underpinning its mission of protecting the Institution's staff, property and information within the framework of Commission Decision (UE, Euratom) 2015/443. It is therefore intended to carry out typical security tasks, including in particular control of access to buildings and to certain restricted access areas within these buildings. Use of the cameras is designed to prevent, detect and document any security incident that occurs in buildings occupied by the Commission or in the

[1] JO L 295, 21.11.2018, p. 39.

Commission européenne/Europese Commissie, 1049 Bruxelles/Brussel, BELGIQUE/BELGIË - Tel. +32 22991111
Office: BERL 03/190 - Tel. direct line +32 229 83936

Bernd.ADOLPH@ec.europa.eu

surrounding area, if this comes under its responsibility (forecourt, car park areas). The term 'security incident' refers in particular to wrongdoing in the form of intrusion, theft, unauthorised access, break-ins, vandalism, assault, threats, and arson.

1.3. Operation

The cameras store all movements in the areas that they monitor, 24 hours a day and 7 days a week, unless otherwise indicated.

1.4. Systematic operational exclusions

The video surveillance system is under no circumstances used to monitor the legitimate activities of staff, service providers or visitors, including the hours they keep, checks on the quality of work and productivity levels.

Similarly, the video surveillance system is not used, even incidentally, to capture or process images in special data categories, such as race, ethnic origin, religious, political or trade union beliefs, and data relating to the health or sexual preferences of individuals.

Places in which individuals clearly consider that their privacy must be protected more strictly, such as bathrooms, waiting rooms, changing rooms or other relaxation areas, cannot be equipped with a video surveillance system.

No webcams for public dissemination of video surveillance footage will be used in the areas covered by this policy.

1.5. Systems not covered by this policy

Video-intercom entry systems, video conference systems, and recording of images for documentary purposes at events such as conferences or training courses are not covered by this text.

2. Installation of video surveillance systems within European Commission buildings

2.1. Analysis prior to installation

If it is planned to install a video surveillance system in a building or site occupied by the European Commission, HR.DS conducts a prior analysis to assess whether use of such equipment is appropriate and proportional to the purpose envisaged, in terms of the number of cameras, their location and the configuration of the system. This analysis may show that, where appropriate, other less intrusive means of protection, such as alarm systems, automated access control, or security doors and windows, would suffice to protect the iInstitution's people, property and information.
The operating schedule and recording arrangements of each system are established in accordance with the same criteria of necessity and proportionality. The same applies to definition of the quality of the camera footage, and therefore to the type of camera selected.
The purpose of this analysis is to reduce the risk of infringing the fundamental rights of any person, particularly with regard to personal data protection and privacy.

If necessary, where required by a specific situation, the Commission's Data Protection Officer (DPO) is consulted.

2.2. Building file

A file is created for each building equipped with video surveillance.

This file lists the type and number of recorders, and the number of active cameras in the building. Each camera is referenced by name, location and a sample image.

2.3. Creation of files

Since numerous Commission buildings are equipped with video surveillance systems that are not standardised and sometimes very old, these files are created gradually according to the resources available.

2.4. Special cases of temporary video surveillance systems

Some investigations relating to matters that are significant in terms of the issue at stake, the value of the damage involved or the risk posed to staff may require the temporary use of discreet and/or intentionally concealed video surveillance systems, which obtain footage of people who are not clearly informed of the surveillance. These systems will be used only as a last resort, when it proves to be impossible to obtain objective evidence by other means to identify the perpetrator(s) of criminal offences (for example, in cases of repeated thefts in the same place, arson, or repeated acts of vandalism).

HR.DS keeps a register of the sites and usage periods involved, as well as the file reference for the relevant investigation.

In each case, HR.DS obtains prior authorisation from the Director-General of DG HR and the Commission's DPO.

3. Installation of cameras

3.1. Field of vision

3.1.1. Outside buildings

In Luxembourg, the installation of cameras outside buildings is conditional on the identification of specific risks, to take account of the obligations deriving from the security agreement between the European Commission and the Luxembourg government, which make the Commission responsible for security around the buildings (and in certain cases, linked extensions and surfaces).

In Brussels, the installation of cameras outside buildings is avoided as far as possible. If a specific risk outside the building is identified, the camera's field of vision does not include public thoroughfares, still less other buildings or private spaces in the vicinity. Nevertheless, when a camera films a part of the building adjacent to the public thoroughfare, a limited amount of this thoroughfare might enter the camera's field of vision. Forecourts belonging to Commission buildings may be filmed in compliance with the principles of this policy.

3.1.2. Inside buildings

The purpose of installing cameras inside buildings is not to monitor the work of staff, working hours or tasks done, or to collect private data. As far as possible, the cameras' field of vision excludes the areas of usual activity of the staff.

Cameras are placed mainly at the entrances and exits of buildings or parts of buildings (entrance halls, vehicle access points, emergency exits, walls or fences surrounding the area under the Commission's responsibility, sites accessible to the public outside the institution), at entrances to restricted areas such as those containing valuable equipment or classified information, and internal areas in buildings, where access rights are differentiated with a view to monitoring by automated access systems.

The goal is to monitor the areas in which incidents jeopardising the security of the Commission's staff, property and information are likely to occur.

3.2. Number of cameras

During the survey prior to installation of a video surveillance system, the number of cameras is examined in order to install as few as possible to achieve the legitimate goal in view.

3.3. Technical specifications of cameras and recording systems

The type of camera is chosen according to the degree of precision required for the goal in view. Most of the cameras used are fixed cameras.

The video surveillance systems are not interconnected with other systems, with the possible exception of a recognition system for vehicle number-plates and drivers entering the car parks of buildings occupied by the Commission.

4. Viewing images

4.1. Live viewing – viewing images recorded less than 24 hours beforehand

Security officers at the entrance to the building can provide live viewing of images to enable immediate monitoring. The screen showing these images is placed in such a way as not to be visible to unauthorised third parties passing nearby. Images may also be viewed remotely, in a control room accessible to staff on duty.

In certain cases, staff on duty may also view footage up to 24 hours old, so that they can react to any dangerous situation or infringement.

4.2. Deferred viewing (images recorded more than 24 hours beforehand)

When the technical equipment allows it, the images filmed may be viewed by authorised officials if justified by a security incident, such as an alarm being set off or a security anomaly being detected (e.g. a door of a building found open, a witness reporting an incident), or as part of an inquiry procedure for duly referenced cases.

4.3. Maintenance staff

The maintenance staff responsible for technical maintenance of the systems have access to all the system components, including recordings, but may not copy images onto any media whatsoever, download them onto independent devices, or transmit them electronically.

4.4. Requests to view images from an individual concerned

An individual, member of staff, service provider, visitor or passer-by who entered into the field of one or more cameras at any time may exercise their right to view the images directly concerning them, and to correct and complete personal data concerning them. However, this right must be strictly limited by the protection of the personal data of third parties who also appear in these images. Therefore, if it is not possible to isolate the images in which the requester alone appears, using standard means and without a disproportionate investment with regard to the importance of the images sought, the individual concerned is informed of the technical reasons making it impossible to provide the images. In addition, in such cases the requester is advised to have the legality of the images concerning him or her checked by the EDPS.

Corrections can only be made by erasing the images in question. This may be done following any legitimate request to erase images that do not constitute objective evidence in the event of an offence, unless there are unforeseen technical obstacles.

A response is given as quickly as possible, and as far as possible within 15 days for any consultation requests. In technically complex cases, unless there are preventing factors as described above, the access authorisation is issued within 90 days of the request being received.

The Commission reserves the right to seek reimbursement of the costs incurred in fulfilling the request from the requester(s), if the amount is kept within reasonable proportions.

4.5. Copying and transferring images to third parties

HR.DS only sends copies of the images it holds to duly authorised administrative or judicial authorities in the framework of investigation cases. The request must be made in writing and precisely delimit the period and the nature of the images requested. An assessment of how necessary the transfer is and whether it is compatible with this policy is carried out to this end.

Aside from the competent judicial authorities, the European Anti-Fraud Office (OLAF) and the Commission's Investigation and Disciplinary Office (IDOC) may obtain such data provided that their representatives are duly authorised to do so. The officials from the Commission's Security Directorate tasked with carrying out investigations, collaborating in them or obtaining evidence may have access footage relating to security incidents, and administrative and/or criminal offences.

5. Recording images

5.1. Place of recording

Images can be recorded either locally in the building equipped with the cameras, or centrally in a technical area in another Commission building.

Recording systems are subject to physical and electronic protection, such that no unauthorised person can view, print or copy the images in any way.

5.2. Access to the systems

Only maintenance staff and those in charge of investigations may access the relevant equipment.

Any failing that may allow or that may have allowed unauthorised access to the data recorded must be notified without delay in writing to the data controller and the Commission's Data Protection Officer (DPO).

5.3. Transmitting images for remote viewing

The persons referred to in point 5.2 above may connect to the system remotely, provided that this is technically possible and that the data is transmitted in a secure manner.

5.4. Length of time for which recorded images are held

Recordings will not be kept beyond the period necessary for achieving the objective of the video surveillance system. Experience shows that requests from judicial authorities and/or the police for access to and/or copies of images as part of an inquiry launched after an offence has been committed generally take a certain amount of time, due to the strict application of the procedures. It is therefore reasonable to set the time limit for holding recorded images at 30 days, by analogy with the Belgian law of 25 May 2018 governing the installation and use of surveillance cameras (Article 6(3)). The systems must be programmed to erase images automatically after this 30-day period. If it is impossible to do this automatically, manual erasing of the footage must be scheduled.

5.5. Removal of decommissioned, obsolete or broken equipment

All equipment or components that contain or have contained video surveillance footage must have all data definitively and irreversibly removed using the safest and most recent techniques, before being decommissioned, removed or designated for destruction so that the data cannot be reconstructed.

6. Publicity

6.1. Posters

Each entrance (entrance halls, vehicle access points) to buildings equipped with cameras and/or recording systems for the images obtained by the cameras is provided with a poster bearing the symbol for a camera and the name and address of the department responsible for processing images, in the customary administrative languages of the Commission and of the host country.

6.2. Website

The reference website, whose address is given on the posters mentioned in point 6.1, contains the most relevant information on this policy. A telephone number and email address are provided, for anyone wishing to obtain further information.

A paper copy of this policy can be obtained on request from HR.DS.

The website also gives the link to the guidelines laid down by the EDPS.

7. Staff training and confidentiality clauses

Any official who has access to video surveillance footage or who has been authorised to carry out work on such images must sign a confidentiality declaration and attend training on personal data protection.

Similarly, staff members of firms supplying security services or maintenance services for video surveillance installations within buildings occupied by the Commission, who are likely to see video surveillance footage, sign a confidentiality declaration and attend training on this subject organised by their firms.

8. Right of appeal

Everybody has the right to have recourse to the European Data Protection Supervisor (edps@edps.europa.eu) if they consider that their rights under Regulation (EU) 2018/1725 have been violated in the processing of their personal data. Before doing so, it is possible to contact the data controller or the Commission's Data Protection Officer.

9. Implementation

The provisions of this policy are monitored and kept under review.

10. Contact point

For any questions or for information on the policy outlined in this document, please contact the Director of the Security Directorate (HR.DS) – Directorate-General for Human Resources and Security (DG HR) – 1049 Brussels – tel.: +32 2299 11 11).

Bernd ADOLPH

Annex: EDPS notification DPR-EC-00654.1, 'Video surveillance – analogue and digital storage'.