EUROPEAN
COURT
OF AUDITORS

European Court of Auditors

Video surveillance policy

DOCUMENT STATUS AND REVISION RECORDS

Document Status

Policy ID	
Classification	Public
Status	
Contact person	Hubert Laligant

Reviewer(s)	**Reviewer(s)**	**Approver(s)**
J. Van Damme		Z. KOLIAS

Revision records

Revision	Date	Who?	Description	Sections affected
Draft	20101112	D. Vavatsis	Initial	All
Revision	2011	J. Van Damme	Review	All
Revision	20140813	J. Van Damme	Update after K3 & K1 building works	All
Revision	20190605	Jo Van Damme Hubert Laligant	Update based on the Secure workplace project	All

TABLE OF CONTENTS

1. INTRODUCTION

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

2. DOCUMENT OBJECTIVES

To document the rules and procedures in place to process the video-surveillance images in accordance with the EDPS guidelines for CCTV, the CCTV guidelines issued by the Luxemburgish data protection authority (CNPD) and Regulation 2018/1725 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data.

3. SCOPE

All video-surveillance systems installed and managed by the ECA within and around its premises located, 12 rue Alcide de Gasperi, 1615 Luxembourg.

4. ENSURANCE

4.1. Revision of the existing system.

A video-surveillance system had already been operating at the ECA before the issuance of the video-surveillance guidelines by the European Data Protection Supervisor ("guidelines") on 17/03/2010. Our procedures, however, have since then been revised to comply with the recommendations set forth in the **Guidelines** (guidelines, section 15). This policy is an update from 2011.

4.2. Self-audit.

The system was subject to a self-audit.

4.3. Data Privacy Impact Assessment.

A data protection-impact assessment (DPIA) was carried out.

A consultation of the EDPS (guidelines, section 4.3) was made on 14/06/2019 and his opinion is outstanding.

Simultaneously with adopting this video-surveillance policy, we also notified the EDPS of our compliance status by sending him a copy of our video-surveillance policy and our audit report.

4.4. Contacts with the relevant data protection authority in the Member State.

The competent data protection authority in Luxemburg (CNPD) was informed and its opinion was asked for the limited surveillance of the direct territory outside the ECA's premises. The CNPD, which has no mandate for EU Institutions, relied on the EDPS opinion which was transmitted to the CNPD. The CNPD was also informed that in particular, both the on-the-spot notice and this video-surveillance policy are also available in French and German, the main official languages of the country.

4.5. Secretary General'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 taken by the ECA's Secretary General after consulting:

- the Director of Human Resources, Finances and General Services, responsible for physical security,
- the ECA's Data Protection Officer, and
- the Staff Committee.

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

4.6. Transparency.

The video-surveillance policy has two versions, a version for restricted use and this public version posted on ECA's internet and intranet sites at the following address: **www.eca.europa.eu/CCTV**. This public version may contain summary information with respect to particular topics or attachments. When this is the case, it is always clearly stated. Information is only omitted from the public version when the preservation of confidentiality is absolutely necessary for compelling reasons (e.g. for security reasons or to preserve the confidentiality of sensitive information or to protect the privacy of individuals).

4.7. Periodic reviews.

A periodic data protection review will be undertaken by the security unit every two years. During the periodic reviews it will be re-assess that:

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

The periodic reviews will also cover all other issues addressed in the first report, in particular, whether the video-surveillance policy still complies with the Regulation and the guidelines (adequacy audit), and whether it is followed in practice (compliance audit).

4.8. Privacy-friendly technological solutions.

Privacy-friendly technological solutions were implemented (see guidelines, section 3.4) by using non-intelligent cameras without sound recording.

5. AREAS UNDER SURVEILLANCE

The video-surveillance system consists of 101 cameras.

No monitoring takes place in any areas under heightened expectations of privacy such as individual offices, leisure areas, toilet facilities and others (see guidelines, section 6.8). The location of the cameras was carefully reviewed to ensure that they minimise the monitoring of areas that are not relevant for the intended purpose (guidelines, section 6.1).

Monitoring outside our building on the territory of Luxembourg is limited to the strict minimum and **covers the immediate surroundings of the premises (buildings and fences) and entrances and exits but does not cover neighbour buildings** as recommended in section 6.5 of the guidelines.

6. PERSONAL INFORMATION COLLECTION AND PURPOSE

6.1. Summary description and detailed technical specifications for the system.

The video-surveillance system is a conventional static system. It records digital image by image. It records pictures taken 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.

6.2. Purpose of the surveillance.

The ECA uses its video-surveillance system for the sole purpose of security and access control. The video-surveillance system helps controlling the access to ECA buildings and ensuring the security of our buildings, the safety of our staff and visitors, as well as property and information located or stored on the premises. It complements the access control system. It is part of the measures supporting our broader security policies and helps preventing, detering, and if necessary, investigating unauthorised physical access, including unauthorised access to secure premises and protected rooms, IT infrastructure, or operational information. In addition, video-surveillance helps preventing, detecting and investigating theft of equipment or assets owned by the ECA, visitors or staff, and threats to the safety of visitors or personnel working at the office (e.g. fire, physical assault).

6.3. 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. It is not used as an investigative tool either (other than investigating physical security incidents such as thefts, unauthorised access or technical malfunctions affecting security devices). 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 7.4 below (see sections 5.7, 5.8 and 10.3 of the guidelines).

6.4. No *ad hoc* surveillance foreseen.

No *ad hoc* surveillance operations are foreseen for which we would need to plan at this time (see guidelines, section 3.5).

6.5. Webcams.

No webcams are installed for video-surveillance (see section 5.10 of the guidelines).

6.6. Special categories of data collected.

No special categories of data are collected (section 6.7 of the guidelines).

7. DATA ACCESS TO DISCLOSURE

7.1. In-house security staff.

Recorded video is accessible to our in-house security staff only. Live video is also accessible to security guards on duty. The security guards have only access to the real time pictures while a limited number of staff from the physical security team are administrators of the system who can grant and revoke access rights and can also view the recorded images, copy, download or delete any of these images.

7.2. Data protection training.

All staff having access rights received a data protection training. Training is provided to each new member of staff and periodic workshops on data protection compliance issues are carried out at least once every two years for all staff with access rights (see section 8.2 of the guidelines).

7.3. Confidentiality undertakings.

At the end of the training, each staff member also signed a confidentiality undertaking.

7.4. Transfers and disclosures.

All transfers and disclosures outside the security team must be formally requested in writing, they must be documented and subject to a rigorous assessment of the necessity of such transfer and the compatibility of the purpose of the transfer with the initial security and access control purpose of the processing (see section 10 of the guidelines). The outline of the register of retention and transfers is included in attachment 6 (see section 10.5 and 7.2 of the guidelines). The DPO is consulted in each case. No access is given to management or human resources.

Local police may be given access if needed to investigate or prosecute criminal offences. Under exceptional circumstances, access may also be granted to the European Anti-fraud Office ("OLAF") in the framework of an investigation carried out by OLAF or those carrying out a formal internal investigation or disciplinary procedure within the Institution, provided that it can be reasonably expected that the transfers may help investigation or prosecution of a sufficiently serious disciplinary offence or a criminal offence. No requests for data mining are accommodated.

7.5. How information is protected and safeguarded?

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.

The ECA's security policy for video-surveillance was established in accordance with section 9 of the EDPS video-surveillance guidelines.

Among others, the following measures are taken:

- secured room, protected by an electronic access control mechanism, where the PC's are hosted for storing the recorded images; dedicated network separated from the ECA's LAN, and no e-mail or any other external connection,
- all staff signed non-disclosure and confidentiality agreements,
- access rights are granted to those resources which are strictly necessary to carry out their jobs only.
- the Physical Security Officer maintains 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 IS THE INFORMATION KEPT?

The images are retained for a maximum of 30 days. Thereafter, all images are physically over-written with the newly recorded images. If an image needs to be stored to further investigation or as an evidence in the framework of a security incident, it may be retained as long as necessary. Its retention is rigorously documented and the need for retention is periodically reviewed. Each retention of images must be notified to the DPO who maintains the retention and transfer register. (see section 7 of the guidelines.)

The system is also monitored live by the security guards at the security control centre 24 hours a day.

9. INFORMATION PROVIDED TO THE PUBLIC.

9.1. Multi-layer approach.

Information to the public about the video-surveillance is provided in an effective and comprehensive manner (see guidelines, section 11). To this end, a multi-layer approach is followed, which consists of a combination of the following methods :

- information panels are placed at the main entrances to the site to alert the public of the existence of monitoring and provide them with essential information on the processing;
- warning labels are placed near the areas monitored;
- this video-surveillance policy is published on the ECA's intranet and internet site;
- print-outs of this video-surveillance policy are also available at our building reception desk and from our security service upon request. A phone number and an email address are provided for further enquiries.

.

9.2. Specific individual notice.

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

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

Provision of notice may sometimes be delayed temporarily, for example, if it is necessary for the prevention, investigation, detection and prosecution of criminal offences. The Institution's DPO is consulted in all such cases to ensure that the individual's rights are respected.

10. VERIFICATION, CORRECTION OR ERASURE OF INFORMATION

Individuals have the right to access information regarding their personal data held by the ECA, and to correct and complete such data. Any request for access of personal data should be directed to the Physical Security Officer (Eca-security@eca.europa.eu; telephone +352 4398 45400). The Data Protection Officer (ECA-Data-Protection@eca.europa.eu; telephone +43 98 4 7777) may also be contacted in case of any other questions relating to the processing of personal data.

Whenever possible, the Security Officer responds to an enquiry in substance within 15 calendar days. If this is not possible, the applicant is informed of the next steps and the reason for the delay within 15 days. Even in the most complex cases access must be granted or a final reasoned response must be provided rejecting the request within three months at

the latest. The Security Officer shall 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 portable media. In case of such a request, the applicants must prove identity (e.g., they should bring an identity document when attending the viewing) and, whenever possible, also designate the date, time, location and circumstances when they were caught on cameras. They must also provide a recent photograph of themselves that allows the security staff to identify them on reviewed images.

At this time, the ECA does not charge applicants for requesting a viewing or a copy of their recorded images. However, the ECA reserves 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 25 of Regulation Council 9296/18 applies in a specific case. For example, following a case-by-case evaluation we may have to conclude that restricting access may be necessary to safeguard the investigation of a criminal offence. A restriction may also be necessary to protect the rights and freedoms of others, for example, when other people are also present on the images, and it is not possible to acquire their consent to the disclosure of their personal data, or to use image editing to remedy the lack of consent.

11. RIGHT OF RECOURSE

Every individual has the right of recourse to the European Data Protection Supervisor (edps@edps.europa.eu) if they consider that their rights under Regulation 2018/1725 have been infringed as a result of the processing of their personal data by the ECA. Before doing so, the ECA recommends that individuals first try to obtain recourse by contacting:

- the Security Officer (Eca-security@eca.europa.eu;), and/or
- the Data Protection Officer (ECA-Data-Protection@eca.europa.eu);

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

12. REFERENCES

Regulation 2018/1725

EDPS CCTV Guidelines

CNPD CCTV guidelines