EUROPEAN COURT OF AUDITORS
Secretariat General

European Court of Auditors

Information Security

Video surveillance policy leaflet

1. INTRODUCTION

For the safety and security of its buildings, assets, staff and visitors, the ECA operates a video surveillance system. The entire video surveillance policy is available at eca.europa.eu/CCTV.

2. ENSURING EFFICIENT TARGETED VIDEO SURVEILLANCE

2.1. Revision of the existing system

The video surveillance system is compliant with the Video surveillance Guidelines issued by the European Data Protection Supervisor ("**Guidelines**") on 17/03/2010.

CNPD, the competent data protection authority in Luxemburg has been informed. In particular, both the notice posted on the spot and this Video surveillance Policy are also available in French and German.

2.2. Privacy-friendly technological solutions

The following privacy-friendly technological solutions have been installed (see **Guidelines**, Section 3.4):

- low resolution cameras
- picture by picture technology

3. AREAS UNDER SURVEILLANCE

The cameras are located at the entry and exit points of the buildings, inside the computer room and in the fitness room.

There are no cameras elsewhere either in the buildings or outside of them. Other than in the fitness room[1], 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 has been carefully reviewed to ensure that they minimise the monitoring of areas that are not relevant for the intended purposes (**Guidelines**, Section 6.1).

Monitoring outside the ECA's buildings on the territory of Luxembourg does not take place, as recommended in Section 6.5 of the **Guidelines**.

4. PERSONAL INFORMATION COLLECTION AND PURPOSE

The video surveillance system is a conventional static system. It makes a digital recording image by image. It records pictures taken by the cameras in the area under surveillance, together with the time, date and location. All cameras operate 24 hours a day, seven days a week. The image quality sometimes allows the identification of those in the camera's area of coverage (see **Guidelines**, Section 6.4). High-tech and

---

[1] A camera has been placed in the fitness room to detect any case of a sole occupant suffering an accident or illness

intelligent video surveillance technologies are not used (see Section 6.9 of the **Guidelines**), the video surveillance system is not connected with other systems (Section 6.10), and covert surveillance (Section 6.11), sound recording and "talking CCTV" are not used (Section 6.12).

The ECA uses its video surveillance system for the sole purposes of safety, security and access control.

The system is not used for any other purpose, nor is it used as an investigative tool (other than for investigating physical security incidents such as thefts or unauthorised access). Only in exceptional circumstances may the images be transferred to investigatory bodies in connection with formal disciplinary or criminal investigation (see Sections 5.7, 5.8 and 10.3 of the Guidelines).

The ECA does not envisage any *ad hoc* surveillance operations requiring advanced planning at this time (see **Guidelines**, Section 3.5).

No webcams are installed for video surveillance (see Section 5.10 of the **Guidelines**).

No special categories of data are collected (Section 6.7 of the **Guidelines**).

5. DATA ACCESS AND DISCLOSURE

5.1. In-house security staff

Recorded images are accessible to staff responsible for physical security only. Live video is also accessible to security guards on duty.

5.2. Data protection training

All personnel with access rights to the video surveillance images have been given data protection training.

5.3. Transfers and disclosures

All transfers and disclosures outside the security unit are documented and subject to a rigorous assessment of the need for these transfers and the compatibility of the purposes of the transfers with the initial security and access control purpose of the system (see Section 10 of the **Guidelines**). The register of retentions and transfers is included in Attachment 6 (see Section 10.5 and 7.2 of the **Guidelines**). As at 28th October 2011, there were no entries in this register. The DPO is consulted in each case. No access is given to management or to the Human Resources Directorate.

5.4. How is information 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.

6. HOW LONG IS THE INFORMATION KEPT?

The images are retained for a maximum of 16 days (7 days at the K8 building). Thereafter, all images are physically over-written with newly recorded images. If any images need 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. Each retention of images must be notified to the DPO, who keeps the retention and transfer register (see Section 7 of the **Guidelines**.)

7. INFORMATION PROVIDED TO THE PUBLIC.

7.1. Specific individual notice

Persons must also be given individual notice if they have been 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 recording is kept beyond the regular retention period,

the recording is transferred outside the security unit, *or*

the identity of the individual is disclosed to anyone outside the security unit.

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

8. VERIFICATION, CORRECTION AND ERASURE OF INFORMATION

Members of the public have the right to access the personal data the ECA hold on them. Any request for access to or the rectification, blocking and/or erasing of personal data should go to the Physical Security Officer (ECA-Security@eca.europa.eu; telephone +352 4398 45911). The Data Protection Officer (ECA-Data-Protection@eca.europa.eu; telephone +352 4398 47777) may also be contacted in the event of any other questions relating to the processing of personal data.

9. RIGHT OF RECOURSE

All persons have the right of recourse to the European Data Protection Supervisor (edps@edps.europa.eu) if they consider that their rights under Regulation 45/2001 have been infringed as a result of the processing of their personal data by the ECA. Before doing so, the ECA recommends that they first contact:

- the Security Officer (see contact details above), and/or
- the Data Protection Officer (ECA-Data-Protection@eca.europa.eu; telephone +352 4398 47777)

10. REFERENCES

Regulation 45/2001

EDPS video-surveillance **Guidelines**