EUROPEAN COURT OF AUDITORS
Secretariat General

European Court of Auditors

Information Security

Video surveillance policy

DOCUMENT STATUS AND REVISION RECORDS

Document Status

Policy ID	
Classification	Court internal
Status	Approved
Contact person	Dimitri Vavatsis

Reviewer(s)	**Reviewer(s)**	**Approver(s)**
J. Van Damme		N. Usher

Revision records

Revision	Date	Who?	Description	Sections affected
Draft	20101112	D. Vavatsis	Initial	All
Revision	20110802	J. Van Damme	Review	All
Approved	20111026	N. Usher	Approved	All

TABLE OF CONTENTS

1. INTRODUCTION

The ECA operates a video surveillance system for the safety and security of its buildings, assets, staff and visitors. This video surveillance policy and its attachments describe the ECA's video surveillance system and the precautions that the ECA takes to protect the personal data, privacy and other fundamental rights and legitimate interests of people filmed by the cameras.

2. DOCUMENT OBJECTIVES

To process the video surveillance 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.

3. SCOPE

All video surveillance systems installed and managed by the ECA in its buildings. The rented buildings K9 and K7, which are managed by the landlord and the Court of Justice, do not fall within the scope of this document.

4. ENSURING EFFICIENT TARGETED VIDEO SURVEILLANCE

4.1. Revision of the existing system

A video surveillance system was already in operation at the ECA before the European Data Protection Supervisor issued the Video surveillance Guidelines ("the Guidelines") on 17/03/2010. However, the ECA's procedures have since been revised so as to comply with the recommendations set out in the Guidelines (Guidelines, Section 15).

4.2. Self-audit

A self-audit has been performed on the system and the relevant report is enclosed as Attachment 1.

4.3. Notification of compliance status to the EDPS

A privacy impact assessment has been performed and is enclosed as Attachment 2.

A prior checking notification has been submitted to the EDPS (Guidelines, Section 4.3) on 26/10/2011 (Attachment 3) and the EDPS Opinion on this notification is enclosed as Attachment 4 (waiting for the Opinion).

At the same time as adopting this video surveillance policy, the ECA also notified the EDPS of its compliance status by sending it a copy of the video surveillance policy and the initial audit report.

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

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

4.5. Secretary General's decision and consultation

The decision to use the current video surveillance system and adopt the safeguards described in this video surveillance policy was made by the ECA's Secretary General after consulting:

- the Director of Finance and Support, 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, was both necessary and proportionate in respect of the purposes described in Section 1 (see Guidelines, Section 5) and addressed the concerns of the DPO and the Staff Committee (see Guidelines, Section 4).

4.6. Transparency

There are two versions of the video surveillance policy, a version for restricted use and this public version, which is available and posted on the ECA's internet and intranet sites at **www.eca.europa.eu/CCTV**. This public version of the Video surveillance policy may contain summary information with respect to particular topics or attachments. Where this is the case, it is always clearly stated. Information is only omitted from the public version where 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).

4.7. Periodic reviews

A periodic data protection review will be undertaken by the security unit every two years, the first by 31 May 2013. These periodic reviews will re-assess that:

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

The periodic reviews will also cover all other issues addressed in the first report, in particular, whether the video surveillance policy continues to comply with the

Regulation and the Guidelines (adequacy audit), and whether it is followed in practice (compliance audit). Copies of the periodic reports will also be included in Attachment 1 to this Video surveillance policy.

4.8. Privacy-friendly technological solutions

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

- low resolution cameras
- picture by picture technology

5. AREAS UNDER SURVEILLANCE

The video-surveillance system consists of 28 cameras. A map with the locations of the cameras is included in Attachment 5 (not added for security reasons).

Of the 16 cameras installed at K1, 13 are located at the building's entry and exit points, including the main entrance, emergency and fire exits and the entrance to the garage. The other three cameras are installed in the garage.

At the K2 building, eight cameras are installed of which five are located at the three entrances and exits, which are protected by an access control system, and at the entrance to the garage. In addition, there are also cameras at the entrance to the computer room, inside the computer room and in the fitness room.

At the K8, four cameras are installed. One at the main entrance, one at each of the two emergency exits and one at the garage entrance.

There are no cameras elsewhere either in the buildings or outside 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 building on the territory of Luxembourg does not take place, as recommended in Section 6.5 of the Guidelines.

6. COLLECTION OF PERSONAL INFORMATION AND PURPOSE

6.1. Summary description and detailed technical specifications for the system

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 will sometimes allow the identification

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

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, therefore, they cannot be used to zoom in on a target or follow individuals around. High-tech or intelligent video surveillance technology 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).

6.2. Purpose of the surveillance

The ECA uses its video surveillance system for the sole purposes of security and access control. The video surveillance system helps control access to ECA buildings and helps ensure the security of its buildings, the safety of its staff and visitors and the property and information located or stored on the premises. It complements the access control system. It forms part of the measures to support the ECA's 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 the theft of equipment or assets owned by the ECA, visitors and staff and threats to the safety of visitors or personnel working at its offices (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 monitor attendance. Neither is the system used as an investigative tool (other than investigating physical security incidents such as thefts or unauthorised access) Only in exceptional circumstances may images be transferred to investigatory bodies in connection with formal disciplinary or criminal investigations such as those 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

The ECA does not envisage any *ad hoc* surveillance operations requiring advanced planning 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 AND DISCLOSURE

7.1. In-house security staff

Recorded video is accessible to the in-house security staff only. Live video is also accessible to security guards on duty. The security guards only have access to the real time pictures, whereas the two staff members responsible for physical security

are the system administrators, who are able to grant and revoke access rights and also view recorded images and copy, download and delete any of these images.

7.2. Data protection training

All personnel with access rights have been given initial data protection training. Training is provided for each new member of the staff and periodic workshops on data protection compliance issues are carried out at least once every two years for all staff with access rights (see Section 8.2 of the Guidelines).

7.3. Confidentiality undertakings

After training, each staff member also signs a confidentiality undertaking.

7.4. Transfers and disclosures

All transfers and disclosures outside the security unit must be formally requested in writing and documented and are subject to a rigorous assessment of the need for the transfer and the compatibility of the purposes of the transfer with the initial security and access control purpose of the system (see Section 10 of the Guidelines). A register of retention and transfers is included as Attachment 6 (empty) (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 given to the European Anti-fraud Office ("OLAF") in connection with an investigation carried out by OLAF itself, the Commission's Investigation and Disciplinary Office ("IDOC") in the context of a disciplinary investigation under the rules set out in Annex IX of the Staff Regulations of Officials of the European Communities, or those carrying out a formal internal investigation or disciplinary procedure within the Institution, provided that it can reasonably be expected that the transfers may help in the investigation or prosecution of a sufficiently serious disciplinary offence or a criminal offence. No requests for data mining are accommodated. For the past five years, for which records of transfers have been held, no transfers have been made for any of the above reasons.

7.5. How is information protected and safeguarded?

A number of technical and organisational measures have been put in place in order to protect the security of the video surveillance system, including personal data.

The ECA's Security Policy for Video surveillance has been drawn up in accordance with Section 9 of the EDPS Video surveillance Guidelines.

Among others, the following measures are taken:

- secure premises, protected by electronic or physical access control, where the PCs used for storing the recorded images are hosted; dedicated network separated from the ECA's LAN, no USB connectivity for the PCs and no e-mail or any other external connection;

- all staff sign non-disclosure and confidentiality agreements;

- users are only granted access rights that are strictly necessary to carry out their jobs.

The Physical Security Officer keeps an up-to-date list of all persons having access to the system at all times, describing their access rights in detail.

8. 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 the 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 periodically reviewed. Each retention must be notified to the DPO, who keeps the retention and transfer register (see Section 7 of the Guidelines).

The system is also monitored live by the security guard at the K1 building reception 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, consisting of a combination of the following two methods:

- on-the-spot notices to alert the public to the fact that monitoring is taking place and provide them with essential information about the processing. This video surveillance policy is published on the ECA's intranet and internet sites;

- print-outs of this video surveillance policy are also available at the building reception desk and from the security unit upon request. A phone number and an email address are provided for further enquiries.

- on-the-spot notices are displayed next to the areas monitored. A notice is displayed at the entrance to the site, the main entrances and the secured rooms.

The ECA's on-the-spot data protection notice is included as Attachment 7.

9.2. Specific individual notice

In addition, individuals 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 *out*side the security unit.

This notification may sometimes be delayed temporarily, for example, if this 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 AND ERASURE OF INFORMATION

Members of the public have the right to access the personal data that the ECA holds on them and correct and supplement such data. Any request for access to or the rectification, blocking and/or erasing 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 +352 4398 47777) may also be contacted in the event 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 of 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 does his/her best to respond earlier, especially if the applicant establishes the urgency of the request.

Where specifically requested, a viewing of the images may be arranged or the applicant may obtain a copy of the recorded images on DVD or other medium. In the event of such a request, the applicants must prove their identity beyond doubt (e.g. they should bring identity cards when attending the viewing) and, whenever possible, also specify the date, time, location and circumstances when they were caught on camera. They must also provide a recent photograph of themselves to allow the security staff to identify them from the images being reviewed.

Currently, the ECA does not charge applicants to view or copy their recorded images. However, it reserves the right to charge a reasonable amount if the number of such access requests increases.

An access request may be refused when an exemption under Article 20(1) of Regulation 45/2001 applies in a specific case. For example, following a case-by-case evaluation, the ECA 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 in the images, and it is not possible to acquire their consent for the disclosure of their personal data or use image editing to remedy the lack of consent.

11. 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 the 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)

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

12. REFERENCES

Regulation 45/2001

EDPS video surveillance Guidelines

EUROPEAN COURT OF AUDITORS
Data Protection Officer

Luxembourg, 19 August 2011
DPO006914EN01-11PP-RELU.doc

Video surveillance audit report

1. INTRODUCTION

1. Since the publication of the EDPS video surveillance guidelines on 17/03/2010, all EU Institutions have been required to carry out an audit of their video surveillance infrastructure and policies and their communication policies vis-à-vis those people subject to the surveillance.

2. The audit was carried out by Mr Johan Van Damme, Data Protection Officer (DPO) at the ECA, and supervised by the the Internal Auditor, Mr Meletios Stavrakis, in the period June – November 2010. The audit was officially notified on 11/06/2010 to the Director of Finance and Support (DFS), who designated Mr Dimitrios Vavatsis, Physical Security Officer (PSO) at the ECA, as the contact person within DFS.

3. In cooperation with the European Parliament's DPO, an audit checklist was created on the basis of the EDPS guidelines.

4. At the beginning of June, the Internal Auditor and the DPO defined the audit programme and methodology and they had an initial meeting with the PSO on 16/06/2010. Further meetings took place on 11 and 30 November 2010.

5. All technical documentation concerning the cameras, the recording system and the software were obtained from the PSO at the beginning of August 2010. All cameras were visited and photographed.

6. The main findings were documented in the IA Internal Audit Note No 01/2001 that was sent on 06/01/2011 to the Secretary-General (Annex 1).

7. The fact that the DPO's audit report was not finalised before the end of December 2010 - a requirement in the guidelines - was due to the termination of the external security company's contract, followed by termination of a second contract with the replacement external company and the insourcing of the physical security activities from 01/04/2011 onwards. These facts required the rewriting of certain parts of the CCTV policy, changes in procedures and a reorganisation of internal staff which resulted in the re-attribution of access rights.

2. SCOPE AND OBJECTIVE

8. Only cameras installed and managed by the ECA (buildings K1, K2 and K8) have been subject to the compliance audit. The cameras managed by the Court of Justice (CoJ) or Property Partners (K9) have been excluded. The reason is that the rented buildings will no longer be used from October 2012 onwards, when their occupants will move to the new extension in K3.

9. The objectives of the compliance audit are to verify how well the ECA has implemented the EDPS guidelines on video surveillance, to identify eventual non-compliances and draw up an action plan if necessary.

3. MANAGEMENT SUMMARY

10. Although the video policy had already been prepared by December 2010, the policy has still not been adopted at the ECA and made publicly available on the Intranet/Internet web site.

11. The current CCTV system is unable to encrypt the transfer and storage of images and is unable to keep an audit log of the handling of the stored images.

12. No procedure exists on what to do if personal data are disclosed to unauthorised people, and how to inform the persons whose personal data have been disclosed.

13. When, in 2012, the current CCTV system is replaced, the call for tender for such a system should specify the "privacy by design" requirement as well as all the technical requirements such a system should meet as laid down in the EDPS's Guidelines.

4. AUDIT FINDINGS AND RECOMMENDATIONS

4.1 Privacy by design

14. The current CCTV system was designed 24 years ago and had very few privacy protection measures built into the system. To meet all the obligations specified in the Guidelines the current system will have to be replaced. In 2012 the new K3 extension of the ECA headquarters will be available to host the staff that are currently located in the rented buildings K7, K8 and K9.

15. Recommendation: In 2012, once K3 has been equipped with a video surveillance system which conforms to the EDPS requirements specified in the guidelines, the existing CCTV system in K1 and K2 should be replaced with a system compatible with the one at K3.

4.2 Privacy impact assessment

16. At the time of the audit no privacy impact assessment concerning the use of a CCTV system had been carried out. A risk analysis to identify if video surveillance was the appropriate measure to reduce the identified risks was carried out but never documented. Both findings are mentionned in the Internal Auditor's Audit Note No1. In the meantime this privacy impact assessment has been carried out and the risk analysis has been documented.

17. The privacy impact assessment demonstrates that video surveillace is justified at the ECA and concludes that the impact is reduced to a minimum.

4.3 Inform the data protection authorities

18. The DPO was notified in 2007 that personal data were handled by staff and the external security company through the video surveillance system.

19. The Luxemburgish national personal data authority was informed in 2011 that a video surveillance system was in operation covering only the site and buildings belonging to the ECA. No Luxemburgish territory is covered.

20. The EDPS was notified with a view to a prior check in 2011, since images may eventually be used during an investigation.

4.4 Decision to use video surveillance

21. The decision to use video surveillance was taken 24 years ago upon a recommendation from the Commission's Security Directorate. In the meantime the risk analysis has shown that video surveillance is the best and most economical solution to prevent physical incidents, to protect assets and staff and assure staff safety in certain areas.

22. In the case of one camera in the stair hall on the ground floor in the K1 building there seems to be no reason to justify its retention.

23. Recommendation: Remove the camera in the stair hall on the ground floor in K1.

4.5 Communication of the video surveillance policy

24. The policy, summary leaflet, the on-the-spot notice and pictograms were available during the audit. Because the policy has still not been adopted, the policy and the summary leaflet are still not available on their dedicated Intranet/Internet pages.

25. Three cameras are not indicated by the ISO camera pictogram.

26. Recommendation: Display the CCTV ISO pictogram in a clearly visible manner at the entrance door of the cafeteria's storage room, the door of the drivers' room and the entrance door to the technical and canteen area.

27. Publish the CCTV policy and its summary leaflet on their dedicated Intranet/Internet pages as soon as the policy is adopted.

4.6 Retention period

28. The retention period for the recorded images has been set at 16 days for the K1 and K2 buildings and 7 days for K8. This is justified by the fact that the ECA closes completely over the Christmas and New Year period and the staff responsible for physical security are unavailable. To permit these people to investigate a physical security incident the images need to be kept for the maximum period the ECA is closed plus five working days to allow searches for images, their copying and/or transfer.

4.7 Areas under surveillance and technology used

29. The areas under surveillance are mainly exit and entry points, access doors or rooms with high value assets and areas where incidents have occurred. Only the fitness room is an exception. Senior management decided to install this camera to replace the supervisor when the contract with the external security company was terminated. Tests showed that sometimes one can recognise people within a distance of six metres from the camera. In all other cases one sees there is a person in the room but one is unable to identify the person. From a privacy point of view this is acceptable. However, the safety reason put forward to justify the installation of the camera is questionable from the point of view of efficacy. If a person in the room is in danger, the security guard should detect this fact as quickly as possible but because the security guards have to supervise many other footages and carry out other tasks at reception there is no guarantee this will happen. On the other hand the saving of €40K per year is another fact senior management used to justify the installation of the camera.

30. The technology used is very privacy friendly as there is no covered surveillance, the system is stand-alone, not interconnected with any other information system, there is no sound recording, no zoom or tracking possibilities, the cameras are low resolution, so there are no face recognition possibilities and only one image per

second is recorded. These are important findings in connection with how well the privacy and personal data of persons captured by the CCTV system are protected.

4.8 Access rights, training and logging capacities.

31. The current system only permits access through a generic user identification for the security guards. This is in order, because the security guards only have access to the live images, they work in a restricted and secured area not accessible by other staff and they perform a 24/7/365 continuous monitoring task to guard the buildings and infrastructure. Connecting each time with their individual user identification at the start of a new working period would be inefficient and makes no sense as a number of staff share the supervisor monitors.

32. The system administrators also shared a generic user identification. After the audit finished each system administrator obtained his own personal user identification.

33. At the time the audit was completed no specific data protection training was offered to the users of the CCTV system. In the meantime all users have been trained in January and August 2011. All users also signed a specific confidentiality statement to protect the personal data handled by them through the CCTV system.

34. The system is unable to log the search, copy and deletion activities. Only logging at the level of the operating system can be activated to identify when the system administrator accesses the system.

35. The stored images are not encrypted to protect the data, should the hard disks which contain the recorded images be stolen or accessed without proper supervision. The current system cannot activate any encryption. However, the data are stored in a proprietary file format which requires specific software to process the images.

36. At K8 the monitors which show the live images from the four cameras are situated in the office of the Logistics secretariat. As the lease on the building terminates in the last quarter of 2012 and no secure place is available, there is no better solution possible. At K1 the monitors with the live images are well situated in a secure area and only accessible by authorised staff.

37. No procedure is available, should CCTV images be disclosed to unauthorised persons, on when and how to inform those whose personal data have been disclosed.

38. Recommendation: In 2012, when K3 is equipped with a video surveillance system, the new system should be able to identify individually each system administrator as well as each individual who can search, copy and/or delete stored images and be able to monitor their activities.

39. The new system should be able to encrypt the stored images.

40. A disclosure procedure needs to be set up.

4.9 Transfer of images.

41. Transfer of images is only possible after having obtained the opinion of the DPO. Transfer of data is only possible in a very limited number of cases for investigations of security incidents, disciplinary or administrative investigations or upon request of law enforcement or national investigating authorities. Transfer is also possible to people who have been victims of a crime or any other incident. Before the transfer is made, each written request will be examined on a case by case basis and may be refused. Senior management or Human Resources have no access to the images. A register containing all transfers was not available at the time the audit was completed but has been created since then.

4.10 Video surveillance policy

42. At the end of the audit the policy and its summary leaflet were available. In the meantime the policy has been modified several times due to the insourcing of the physical security function, numerous organisational changes and the rescheduling of certain tasks to other organisational units.

43. However, the policy had still not been adopted by mid-August, but the services concerned are aware of the policy and its impact and they respect it fully.

44. Recommendation: The ECA should adopt without delay the video surveillance policy to comply with the EDPS's Guidelines, and to be able to communicate it to the public and all those who may be captured by the CCTV system.

Action plan

Action No	Action	Deadline
1	Replace current CCTV system when the K3 CCTV system is installed	01/10/2012
2	Remove the camera in the stair hall, ground floor, K1	03/10/2011
3	Display 3 CCTV pictograms at the garage	19/09/2011
4	Publish the CCTV policy and its summary leaflet on their dedicated Intranet/Internet pages	03/10/2011
5	Draw up a disclosure procedure	07/11/2011
6	Adopt the video surveillance policy	03/10/2011

EUROPEAN COURT OF AUDITORS

DATA PROTECTION OFFICER

Privacy Impact Assessment (PIA)

Video surveillance

(13/07/2011)

Overview

The overview should include:

- The system's technical name and the name by which it is commonly referred to and the person responsible for its implementation and oversight.
- The objective of the CCTV.
- A general description of the technology and the system.
    - Technology: for example, a description of the camera and recording technologies, with model numbers, vendors, and functions.
    - System: for example, a description of the network of surveillance devices - where and how they are installed, the number of devices, the system for collecting and, if applicable, monitoring the visual information.

A clear and concise overview provides the reader with the context in which to view the remainder of the PIA.

The video surveillance system installed in the K1 and K8 buildings dates back to 1988 and has been gradually expanded with more cameras. The primary system is a Geutebuck system with 9 low resolution cameras connected via a bus network taking black and white images at the rate of one every second. This system was supplemented by a second Geutebuck system connected to a Multiscope image recording system with low resolution colour cameras over an IP-network.

The Physical Security Officer is responsible for the video surveillance system.

Video surveillance in the K7 building is the responsibility of the Court of Justice as the ECA only rents part of the building.

The video surveillance in the K9 building is the responsibility of the building owner and is controlled by a private security company with whom the ECA has no relation or contract.

The video surveillance of the "Antenna" in Brussels is the responsibility of the European Parliament as the ECA rents only part of the top floor.

The objective of the video surveillance is mainly to monitor access to the ECA's premises and buildings in the interest of security and to protect certain valuable assets.

In K1 there are 15 cameras installed: one for every external door, around the building, the entrance to the premises and 1 in the stairs hall on the ground floor.

In K2 there are 9 cameras installed: one on every entrance door, one at the entrance door of the computer room, one inside the computer room and one in the fitness room.

In K8 4 cameras are installed at every external entrance door.

The camera views (for K1-K2) are visualised at the reception/security area in K1 in real time and only 2 staff members have the access rights to search through the recorded images. The PC which can access the recorded images is located in a protected area with limited access rights and the PC is protected by user-id/password.

The camera views for K8 are available at the Logistics secretariat and used to open the doors in case a visitor wants to enter the building. The PC which can access the recorded images is located in a locked technical room with limited access rights and the PC is protected by user-id/password. No images can be extracted.

1 The System and the Information Collected and Stored Within the System

The following questions are intended to define the scope of the information collected, as well as the reasons for its collection as part of the strategy being developed. The term "information" includes all images and footage captured by the camera system and any information associated with those images that can be linked to individuals. If the images are viewed but not stored, please indicate that process below.

1.1 What information is to be collected?

(Please check the following if applicable)
The System's technology enables it to record:

Video

Static Range: between 3 and 20 meters
~~Zoom Range:~~
~~Pan from one angle to another~~:

~~Tracking~~

~~Automatic (for example, triggered by certain movements, indicators)~~
~~Manual (controlled by a human operator)~~

~~Sound~~

~~Frequency Range:~~

Provide a description of what the camera is intended to view.

The System typically records:

~~Passersby on public streets.~~
~~Textual information (such as license plate numbers, street and business names, or text written on recorded persons' belongings).~~
~~Images not ordinarily available to a police officer on the street:~~
~~Inside commercial buildings, private homes, etc.~~
~~Above the ground floor of buildings, private homes, etc.~~
~~The System does not record or store the images~~.
Passers-by at entrance doors/ECA premises
Passers-by in the stair hall
Fitness room users
Computer room visitors

1.1.1 If the activity seeks any specific information or types of information, please specify what is being sought.

NA

1.1.2 Is the information obtained from the CCTV monitoring combined with any other information; and if so, please describe the other information.

NO

1.2 From whom is the information collected?

General public in the monitored areas.
Targeted populations, areas, or activities (please describe). Fitness room users + computer room visitors
~~Security personnel are directed to focus on particular people, activities, or places.~~

1.2.1 Describe any training, guidance, or policies given to security responsible staff that direct them to focus on particular people, activities, or places.

Over a number of sessions, management staff responsible for physical security have been informed of what the EDPS guidelines mean and that video surveillance can be very privacy intrusive, how this could be reduced and that duly justified reasons should be presented to be able to continue with video surveillance and/or targeted video surveillance.

1.3 Why is the information being collected? Identify all that apply.

~~For traffic-control purposes~~
Crime prevention
Crime detection
To aid criminal enquiries
Threat identification
~~Terrorism investigation~~
~~Terrorism prevention~~
~~Other (please specify)~~

1.3.1 Policy Rationale

Provide a brief description stating why cameras are necessary for the organisation. Description may address one or more of the following:

Crime prevention rationale: For example: (1) crimes in-progress may only be prevented if the cameras are monitored in real-time. (2) a clearly visible camera alerting the public that they are monitored may deter criminal activity, at least in the monitored area.
Crime investigation rationale: For example: a hidden camera may be investigative, providing after-the-fact records of persons and locations that may be subpoenaed.
Terrorism rationale: For example: video footage is collected to compare against information contained in terrorist databases.

The main reason is access control when the security guards are requested to open the gate, doors, and garage; secondly, to detect possible intrusion attempts; thirdly, for crime prevention. In the fitness room, to establish whether persons exercising on their own have suffered an accident or malaise. Furthermore, to provide information during a criminal enquiry.

1.3.2

Detail why the particular cameras, their specific placement, the exact monitoring system and its technological features were selected. For example, describe how low-light technology was selected to combat illegal border crossing at night. It is not sufficient to merely state the general purpose of the system.

The system was selected in 1987 when the ECA's main building was constructed. The low resolution cameras and easy-to-use system were selected

for their excellent price/quality relationship and robustness. They were also selected to limit the privacy impact (no infrared, no sound recording, no tracking possibilities, no zooming feature).

1.3.3 Are you using the cameras to track and/or to identify individuals?

NO

1.4 How is the information collected?

~~Real-time monitoring, with footage streamed, but not stored.~~
Real-time monitoring with footage stored.
~~Footage not monitored, only stored.~~

1.5 Operating Policies and Procedure

Describe the policies governing how the records can be deleted, altered or enhanced, either before or after storage. Are there access control policies limiting who can see and use the video images and for what purposes? Are there auditing mechanisms to monitor who accesses the records, and to track their uses, and if so, are these mechanisms a permanent and unalterable part of the entire system? What training was conducted for officials monitoring or accessing the technology?

The recorded images are written in a cyclic way (when the maximum number of days of storage has been reached, new images overwrite the old) on the hard disk of the video surveillance system. In the K8 system, the hard disk is so small that the foreseen maximum conservation date is never reached. Recorded images cannot be altered or enhanced.

Only the physical security officer (and his deputy) can access the recorded images. The rules on when they can access these images are specified in the video surveillance policy.

Permanent audit actions are activated on the use of the dedicated PC which can access the recorded images but no audit mechanisms are available in the viewing software (> 23 years old).

The physical security staff who can access the recorded images have been informed by the ECA's DPO about the CCTV guidelines and general principles of Data Protection.

1.6 Effectiveness

Describe how the organisation will evaluate the camera system's performance. Are there specific metrics established for evaluation? Is there a specific timeline for evaluation?

During the process of achieving compliance with the EDPS's CCTV guidelines the ECA has evaluated the performance of CCTV systems and will repeat the exercise before selecting the CCTV system for the new building extension that is planned to be ready by October 2012.

1.7 Cost Comparison

Has the organisation done a cost comparison of the camera system with alternative means of addressing the system's purposes that may have less of an impact on privacy? If so, provide a summary of such cost comparison (for example, compare the cost of the camera system to adding law enforcement personnel to patrol the area.)

Yes, this comparison has been made and the current CCTV systems have cost the ECA 0 € (zero) since installation. If these cameras were to be replaced by security staff to verify, every time someone presents himself/herself at an entrance door, whether that person represents a potential threat, an additional 8 security staff would be required at a cost of 40 000 euro per year per security guard.

1.8 What specific legal authorities, arrangements, and/or agreements govern the camera system?

The section should include a description of the legislative authorisation for EU Institutions, Agencies and Bodies, as well as any executive or law enforcement decision authorising the system. In addition, provide a list of the limitations or regulations controlling the use of the camera system. This may include existing law enforcement standards, such as subpoenas and warrants, or surveillance-specific rules. For example, is a warrant required for tracking or identifying an individual?

Reg 45/2001
EDPS CCTV guidelines
The EDPS will be the control authority.
The ECA's DPO will perform an annual audit of the CCTV system.

1.9 The Decision Making Process

Describe the decision making process that led to the purchase of the camera system.
Decision making process included public comment or review
The process relied on:

~~case studies~~
~~research~~
~~hearings~~
~~recommendations from camera vendors~~
~~information from other localities~~
other (please specify)

Commission's security directorate was consulted in 1987 to establish which CCTV system was required for the ECA building

1.10 Privacy Impact Analysis

Given the amount and type of data collected, and the system's structure, purpose and use, discuss what privacy risks were identified and how they were mitigated. If, during the system design or technology selection process, decisions were made to limit the scope of surveillance or increase accountability, include a discussion of this decision.
Relevant privacy risks you can discuss include:

- **Privacy rights**. For example, cameras can capture individuals entering places or engaging in activities where they do not expect to be identified or tracked. Such situations may include entering a doctor's office, or an Alcoholics Anonymous, social, political, or religious meeting.
- **Freedom of speech and association**. Cameras may give the government records of what individuals say, do, and read in the public arena, for example documenting the individuals at a particular rally or associations between individuals. Such recording may chill constitutionally-protected expression and association.

- **Government accountability and procedural safeguards**. While the expectation is that law enforcement and other authorised personnel will use the technology legitimately, the design should anticipate and safeguard against unauthorised uses, including creating a system of accountability for all uses.
- **Equal protection and discrimination**. Government surveillance, because it makes some policing activities invisible to the public, poses heightened risks of misuse, such as profiling by race, citizenship status, gender, age, socioeconomic level, sexual orientation, or otherwise. Decisions about camera placement, and dynamic decisions about camera operation, should be the product of rationale, non-discriminatory processes and inputs. System decisions should be scrutinized with fairness and non-discrimination concerns in mind.

  Only low resolution pictures from each camera, which are saved at a frequency of one picture per second. These recorded images can only be accessed from a PC located in a protected area which is protected by a user-id and password. For its purpose and use see point 1.3.1.

  The only privacy impact which was identified concerns the camera installed in the fitness room, which can identify the persons exercising up to a distance of 5 metres from the camera. The Staff Committee has asked questions about the appropriateness of this camera and if the full-time presence of a fitness trainer/security guard is not a better alternative.

2 – Uses of the System and Information

2.1 Describe uses of the footage or images derived from the cameras.

Please describe in detail how the footage or images are used, as well as how the footage or images may be used in the future.

Between 3 and 20 metres and as described in 1.3.1.

No changes foreseen for the future.

2.2 Privacy Impact Analysis

Describe any types of controls that are in place to ensure that the footage or images are handled in accordance with the above-described uses. For example, is appropriate use of the information covered in training for all users of the system? Are audit logs regularly reviewed? What disciplinary measures are in place if an individual is found to be inappropriately using the technology or records?

Only 2 users can access the system, log files are controlled once a year or if an incident occurs or if there are doubts concerning the proper use of the system.

The disciplinary measures in place are specified in the staff regulation on inappropriate use or divulgation of information obtained during the performance of the official's tasks and duties.

3 – Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What is the retention period for the information in the system (i.e., how long are footage or images stored)?

~~24-72 hours~~
~~72 hours – 1 week~~
~~1 week – 1 month~~
~~1 month – 3 months~~
~~3 months – 6 months~~
~~6 months – 1 year~~
~~more than 1 year (please describe)~~
~~indefinitely~~
16 days to be able to cover the maximum period the ECA is closed (Christmas + New Year) + 5 working days

3.1.1 Describe any exemptions for the retention period (i.e. part of an investigation or review)

During an administrative or disciplinary investigation the images related to the facts investigated could be retained as long as the disciplinary procedure takes place + the period foreseen for appeal

3.2 Retention Procedure

Footage or images are automatically deleted after the retention period expires
~~System operator required to initiate deletion~~
~~Under certain circumstances, officials may override detention period:~~
~~To delete the footage or images before the detention period~~
~~To retain the footage or images after the detention period~~
~~Please describe the circumstances and official process for override~~

3.3 Privacy Impact Analysis:

Considering the purpose for retaining the information, explain why the information is maintained for the designated period.

The retention period of 16 days is to permit the staff responsible for physical security, who can access the recorded images, to review an incident. As the ECA is closed during the Christmas – New Year period, those staff are not then present at the ECA. A period of 5 working days has been added to the closing period to permit the physical security staff to access the recorded images.

4 – Internal Sharing and Disclosure

The following questions are intended to describe the scope of sharing *within* the organisation's operation. *External sharing with outside entities will be addressed in the next section.*

4.1 With what internal entities and types of personnel will the information be shared?

Internal Entities
~~Investigators~~
~~Internal audit unit~~
~~Financial unit~~
~~Physical security unit~~
~~Other (please specify)~~
~~None~~

~~Types of Personnel~~
~~Command staff (please specify which positions)~~
~~Middle management (please specify)~~
~~Entry-level employees~~
~~Other (please specify)~~

4.2 For the internal entities listed above, what is the extent of the access each receives (i.e. what records or technology is available to them, and for what purpose)?

In the presence of the physical security officer they may search, view, extract and, if necessary, print the images.

4.2.1 Is there a written policy governing how access is granted?

~~No~~
Yes (please detail)
Specified in CCTV policy

4.2.2 Is the grant of access specifically authorised by:

~~Statute (please specify which statute)~~
~~Regulation (please specify which regulation)~~
Other (please describe): Investigation procedures.
~~None~~

4.3 How is the information shared?

4.3.1 Can personnel with access obtain the information:

~~Off-site, from a remote server~~
Via copies of the video distributed to those who need it
Only by viewing the video on-site
Other (please specify): see point 4.2

4.4 Privacy Impact Analysis:

Considering the extent of internal information sharing, discuss what privacy risks were identified and how they were mitigated. For example, discuss any access controls, encryption, training, regulations, or disciplinary procedures that will ensure only legitimate uses of the system within the department.

Information gathered for investigations is always treated with the highest possible level of security and confidentiality, locked away in secure places and treated on PC's not connected to the network. No training has been given to investigators.

5 – External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to your operation – including other EU organisations, National agencies, authorities, as well as private entities and individuals.

5.1 With which external entities is the information shared?

List the name(s) of the external entities with whom the footage or images and related information will be shared. The term "external entities" refers to individuals or groups outside your organisation.

~~Local government agencies (please specify)~~
~~National agencies (please specify)~~
~~EU organisations (please specify)~~
~~Private entities:~~
~~Businesses in monitored areas~~
~~Insurance companies~~
~~News outlets~~
Other (please specify) If a criminal act has taken place and the proof of the act(s) is on the film or one could identify the authors of such acts, the recorded images could be handed over to national police authorities.

Individuals:

~~Crime victims~~
~~Criminal defendants~~
~~Civil litigants~~
~~General public~~
~~Other (please specify)~~

5.2 What information is shared and for what purpose?

5.2.1 For each entity or individual listed above, please describe all of the following:

The purpose for disclosure: Criminal investigations
The rules and regulations governing disclosure: Upon presentation of a mandate delivered by the "Procureur"(State Prosecutor)
Conditions under which information will not be disclosed: N/A but see 5.3
Citations to any specific authority authorizing sharing of the camera footage or images: N/A

5.3 How is the information transmitted or disclosed to external entities?

Discrete portions of camera footage or images are shared on a case-by-case basis
~~Certain external entities have direct access to camera footage or images~~
~~Real-time feeds of footage or images between agencies or departments~~
~~Footage or images are transmitted wirelessly or downloaded from a server~~
~~Footage or images are transmitted via hard copy~~
~~Footage or images may only be accessed on-site~~

5.4 Is a Memorandum of Understanding (MOU), contract, or agreement in place with each external organisation with whom information is shared, and does the MOU reflect the scope of the information currently shared?

~~Yes~~
No

If an MOU is not in place, explain steps taken to address this omission.
Police forces need to follow a strict protocol when entering EU Institutions and when information is requested they need to present an official request from a "procureur".

5.5 How is the shared information secured by the recipient?

For each interface with a system outside your operation:
~~There is a written policy defining how security is to be maintained during the information sharing~~
~~One person is in charge of ensuring the system remains secure during the information sharing (please specify)~~
~~The external entity has the right to further disclose the information to other entities~~
~~The external entity does not have the right to further disclose the information to other entities~~
~~Technological protections such as blocking, face-blurring or access tracking remain intact one information is shared~~
~~Technological protections do not remain intact once information is shared~~
The Luxemburgish police have their own strict rules on what information can be disclosed or not.

5.6 Privacy Impact Analysis:

Given the external sharing, what privacy risks were identified? Describe how they were mitigated. For example, if a sharing agreement is in place, what safeguards (including training, access control or assurance of technological privacy protection) have been implemented to ensure information is used appropriately by outside agents?

It's the responsibility of the police.

6 – Technical Access and Security

6.1 Who will be able to delete, alter or enhance records either before or after storage?

~~Operation personnel~~
~~Persons who will have routine or ongoing access to the system (please specify)~~
Other (please specify): In principle it is not possible to delete, alter or enhance.

6.1.1 Are different levels of access granted according to the position of the user? If so, please describe.

~~All authorized users have access to real-time footage or images~~
~~Only certain authorized users have access to real-time footage or images (please specify which users)~~
~~All authorized users have access to stored footage or images~~
~~Only certain users have access to stored footage or images (please specify which users)~~
~~All authorized users can control the camera functions (pan, tilt, zoom)~~
~~Only certain authorized users can control the camera functions~~
~~All authorized users can delete or modify footage or images Only certain authorized users can delete or modify footage or images (please specify which users)~~
Only security guards can view real time images. Only 2 persons can access the recorded images.

6.1.2 Are there written procedures for granting access to users for the first time?

~~Yes (please specify)~~
No

6.1.3 When access is granted:

~~There are ways to limit access to the relevant records or technology (please specify)~~
There are no ways to limit access

6.1.4 Are there auditing mechanisms:

~~To monitor who accesses the records?~~
~~To track their uses?~~

6.1.5 Training received by prospective users includes discussion of:

Liability issues
Privacy issues
Technical aspects of the system
Limits on system uses
Disciplinary procedures
~~Other (specify)~~

~~No training~~

The training lasts:

~~None~~

0-1 hours

~~1-5 hours~~

~~5-10 hours~~

~~10-40 hours~~

~~40-80 hours~~

~~More than 80 hours~~

The training consists of:

~~A course~~

~~A video~~

~~Written materials~~

~~Written materials, but no verbal instruction~~

~~None~~

Other (please specify): First of all short explanations of regulations and then question and answer.

6.2 The system is audited:

~~When an employee with access leaves the organization~~

If an employee is disciplined for improper use of the system

~~Once a week~~

~~Once a month~~

Once a year

~~Never~~

When called for

6.2.1 System auditing is:

Performed by someone within the organisation: DPO

~~Performed by someone outside the organization~~

Overseen by an outside body (for example a city council or other elected body – please specify): EDPS

6.3 Privacy Impact Analysis:

Given the sensitivity and scope of information collected, what privacy risks related to security were identified and mitigated?

The only privacy risk which was identified is the fact that the images recorded by the camera installed in the fitness room, which can identify the persons exercising within 5 metres of the camera, could be used to spy on these sports enthusiasts.

The risk was considered to be acceptable by senior management.

7 – Notice

7.1 Is notice provided to potential subjects of camera recording that they are within view of a camera?

Signs posted in public areas inform the public of recording by cameras
Notice in multiple languages
Attached is a copy of the wording of such notice
"For your safety and security, this building and its immediate vicinity is under video surveillance. Recordings are retained for 16 days.
For further information, please consult eca.europa.eu/cctv or contact the ECA's security unit at +352 4398 1 or ECA-security@eca.europa.eu"
~~Notice is not provided~~
~~Other (please describe)~~

8 – Technology

The following questions are directed at analysing the selection process for any technologies used by the camera system, including cameras, lenses, and recording and storage equipment.

8.1 Were competing technologies evaluated to compare their ability to achieve system goals, including privacy protection?

Yes
~~No~~

8.2 What design choices were made to enhance privacy?

~~The system includes face-blurring technology~~
~~The system includes blocking technology~~
~~The system limited location to address privacy~~
The system has other privacy-enhancing technology (Please specify)
Stored images with low resolution
No zooming and tracking possibilities, fixed cameras, mostly b/w
Only image per image storage every second
~~None (Please specify)~~

9 – Attachments to the PIA

~~Authorising legislation~~
~~Grant documents~~
~~Transcript of public hearing or legislative session~~
~~Program manuals outlining the system's rules and regulations~~
~~Other (please specify)~~

Physical Security Officer Signature

Dimitrios Vavatsis

Data Protection Officer Signature

Johan Van Damme

_____

To be filled out in the EDPS' office

NUMERO DE REGISTRE:

NOTIFICATION DE CONTRÔLE PREALABLE

Date de soumission :

Numéro de dossier :

Institution :

Base légale : article 27-5 du Règlement CE 45/2001(1)

(1) OJ L 8, 12.01.2001

INFORMATIONS NECESSAIRES (2)

(2) Merci de joindre tout document utile

1/ Nom et adresse du responsable du traitement
Cour des comptes européenne
12 rue Alcide de Gasperi
L-1615 Luxembourg

2/ Services de l'institution ou de l'organe chargés du traitement de données à caractère personnel
Cellule sécurité physique & réception - Unité Logistique - Direction Finances et Soutien

3/ Intitulé du traitement
Vidéosurveillance

4/ La ou les finalités du traitement
Contrôle d'accès des bâtiments et certaines locaux
Prévention à l'intrusion et criminalité
Protection des biens et personnes
Comme outil dans la sauvegarde des gens victime d'un indicent ou malaise à la salle du fitness.
Utilisé comme une preuve éventuelle aux cour des investigations.

5/ Description de la catégorie ou des catégories de personnes concernées
Des gens qui entrent et quittent des bâtiments.
Certaines utilisateurs de la salle de fitness
Des gens qui entrent dans la salle des serveurs.

6/ Description des données ou des catégories de données *(en incluant, si nécessaire, les catégories particulières de données (article 10) et/ou l'origine des données)*

Images des gens et voitures qui entrent et sortent le site et/ou les bâtiments ainsi la salle des serveurs et certaines utilisateurs de la salle fitness.

7/ Informations destinées aux personnes concernées

Pictogrammes à l'entrée du site et à plusieurs portes, notification en 3 langues (FR, DE, EN) à chaque entrée des bâtiments, politique de vidéosurveillance disponible sur Intranet/Internet de la Cour.

8/ Procédures garantissant les droits des personnes concernées*(droits d'accès, de faire rectifier, de faire verrouiller, de faire effacer, d'opposition)*

Les personnes filmées peuvent faire une demande auprès la sécurité physique ou le DPO pour consulter les images auxquelles ils se trouvent.
Il n'y a pas moyen de demander la rectification, le verrouillage, l'effacement des images ou faire opposition d'être filmé (sauf à ne pas entrer aux endroits qui sont couvert par les cameras).

9/ Procédures de traitement automatisées / manuelles
Le traitement est entièrement automatisé: du capture jusqu'au effacement des images.

10/ Support de stockage des données
Les images sont stockées en format digitalisé sur les disques durs du PC/enregistreur.

11/ Base légale et licéité du traitement

Décision du management en 1988 d'installer un système de vidéosurveillance au bâtiment de la Cour
Politique de vidéosurveillance.

12/ Destinataires ou catégories de destinataires auxquels les données sont susceptibles d'être

Responsables pour la sécurité physique et gardiens de sécurité.
Police au autre services d'investigations.
Les personnes victime d'un incident physique ou d'une crime.
Des investigateurs des investigations administratives/disciplinaires

13/ Politique de conservation des données personnelles (ou catégories de données)

Les images sont sauvegardé 16 jours au bâtiment principal (K1 & K2) et sept jours au bâtiment K8.

13 a/ Dates limites pour le verrouillage et l'effacement des différentes catégories de données
(après requête légitime de la personne concernée)
(Merci d'indiquer les dates limites pour chaque catégorie, si nécessaire)

N/A

14/ Finalités historiques, statistiques ou scientifiques
Si vous conservez les données pour des périodes plus longues que celles mentionnées ci-dessus, merci d'indiquer, si nécessaire, ce pourquoi les données doivent être conservées sous une forme permettant l'identification.

N/A

15/ Transferts de données envisagés à destination de pays tiers ou d'organisations internationales

N/A

16/ Le traitement présente des risques particuliers qui justifient un contrôle préalable :(Merci de décrire le traitement):

Comme spécifié dand les lignes directrices du CEPD un contrôle préalable est nécessaire au moment que les images peuvent être utilisés pendants une investigation ne pas causé par un incident physique.

comme prévu à:

XArticle 27.2.(a)
Les traitements de données relatives à la santé et les traitements de données relatives à des suspicions, infractions, condamnations pénales ou mesures de sûreté,

Article 27.2.(b)
Les traitements destinés à évaluer des aspects de la personnalité des personnes concernées, tels que leur compétence, leur rendement ou leur comportement,

□ Article 27.2.(c)

L*es traitements permettant des interconnexions non prévues en vertu de la législation nationale ou communautaire entre des données traitées pour des finalités différentes,*

□ Article 27.2.(d)

Les traitements visant à exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat,

□ Autre (concept général de l'article 27.1)

17/ Commentaires

18/ Mesures prises pour assurer la sécurité du traitement *(3)*
Merci de vérifier tous les points de l'article 22 du règlement (CE) 45/2001.
3) Ne sera pas publié dans le registre du CEPD (article 27.5 du règlement (CE) 45/2001)

LIEU ET DATE: Luxembourg 08/08/2011

DELEGUE A LA PROTECTION DES DONNEES: Johan VAN DAMME

INSTITUTION OU ORGANE COMMUNAUTAIRE: Cour des comptes européenne

To be filled out in the EDPS' office

AVIS DU CEPD

Suivi *(en cas de mesures à prendre)*

VIDÉOSURVEILLANCE

Pour votre sécurité, ce bâtiment et son voisinage immédiat sont placés sous vidéosurveillance. Les images sont conservées pendant 16 jours.

Pour de plus amples informations, veuillez consulter la page eca.europa.eu/cctv ou prendre contact avec l'unité de sécurité de la CdCE en téléphonant au +352 4398 1 ou en adressant un courriel à

ECA-security@eca.europa.eu.

Les badges doivent être portés de manière visible

VIDEOÜBERWACHUNG

Zu Ihrer Sicherheit werden dieses Gebäude und seine unmittelbare Umgebung videoüberwacht. Die Aufnahmen werden 16 Tage lang gespeichert.

Weitere Auskünfte erhalten Sie unter der Adresse www.eca.europa.eu/cctv.

Sie können sich aber auch mit der Sicherheitsabteilung des ERH unter +352 4398 1 oder

ECA-security@eca.europa.eu

in Verbindung setzen.

Ausweise müssen sichtbar getragen werden

VIDEO SURVEILLANCE

For your safety and security, this building and its immediate vicinity is under video-surveillance. Recordings are retained for 16 days.

For further information, please consult eca.europa.eu/cctv or contact the ECA's security unit at +352 4398 1 or ECA-security@eca.europa.eu.

Badges must be worn visibly