European Investment Bank Group

Video-surveillance policy

European Investment Bank Group

TABLE OF CONTENTS

1. Purpose and scope of the video-surveillance policy

This document sets out the policy for managing the Banks's video-surveillance systems in the light of its security requirements and constraints and in conformity with the relevant texts, namely (i) Regulation No 45/2001 of 18 December 2000 (**"the Regulation"**) and (ii) the Guidelines published by the European Data Protection Supervisor ("**the EDPS"**) dated 17 March 2010, the aim of which is to minimise the impact of video-surveillance on privacy and other fundamental rights.

2. Respect for privacy, data protection and compliance with the relevant rules

2.1. Compliance status

The Security and Services Unit within the Facilities Management Division (i) designs the video-surveillance systems to meet the Bank's security needs, (ii) ensures that the equipment and the system in general is in line with the recommendations of the EDPS and (iii) directs and manages the coordination between the various stakeholders.

2.2. Audit

Whenever there is any substantial change in the system, the Bank carries out an audit and an analysis of the impact of these changes. In every case, the Bank's Data Protection Officer ("DPO") and the Staff Representation via the Joint Committee on Risk Prevention and Protection at Work ("CPPPT") are involved from the outset in these processes.

2.3. Notification of the compliance status to the EDPS

In view of the limited deployment of the system, the Bank has not deemed it necessary to carry out an impact analysis or to submit to the EDPS a prior checking notification in respect of the existing installations.

When this video-surveillance policy was adopted we notified our compliance status to the EDPS, sending a copy of our video-surveillance policy and of the audit report.

2.4. The decision to install video-surveillance at the EIB

Video-surveillance was installed as part of the overall effort to ensure security in the buildings of the EIB's Headquarters.

2.5. Transparency

There are two versions of the video-surveillance policy: a version for restricted use and this public version. The public version can be consulted on our intranet and on our websites at the following addresses: http://www.eib.org/ and http://www.eif.org/ .
This public version of the video-surveillance policy sets out the main elements of the Bank's general policy in this area. For security reasons, some confidential information is not included in this document but may be consulted on request.

In addition, notices are displayed at the reception desks and in the buildings to inform users and visitors that the Bank's premises are under video-surveillance.

2.6. Periodic reviews

An examination of the video-surveillance systems is carried out by the Security and Services Unit every two years, the next one being scheduled for no later than September 2013. On the occasion of these periodic reviews, an examination is made of:

- the usefulness of the video-surveillance system;
- its suitability for the purposes for which it was designed;
- the possible existence of appropriate alternatives.

The periodic reviews are designed to verify in particular whether the video-surveillance policy is still in compliance with the Regulation and the Guidelines. These audits are carried out by specialist external firms.

2.7. Privacy-friendly technological solutions

The main technical solutions employed to promote respect for privacy reflect the following two main principles:

- camera locations and camera viewing angles are fixed so as to film only the private areas (the EIB site). Furthermore, those parts of the buildings where there are heightened privacy expectations (e.g. offices, leisure areas, toilet facilities, changing rooms, etc.) are not monitored by video-surveillance cameras.
- Access to the recorded data is password-protected and is available only to the person responsible for data processing, namely the official in charge of the Bank's Security and Services Unit. He can delegate these rights to a designated person.

3. Areas under video-surveillance

In order to protect property and to ensure the safety of staff and visitors, the following areas are under video-surveillance:

- the areas where sensitive information or high-value items are kept or where there is other property which requires enhanced protection for a very specific reason;
- building entrances and exits (including emergency exits and the walls and fences surrounding the buildings or the site);
- the entrances and exits of various parts of a building subject to different access regimes and separated by security doors or other access control mechanisms.

4. Type of personal data collected and purpose

4.1. Summary description and technical specifications of the system

Each of the Bank's buildings is fitted with a video-surveillance system. Each system is designed according to the same principle. The only variable is the quantity of equipment (cameras, recorders) depending on the size of the site and the security requirements.
Given that each building is fitted with its own system, the images from the cameras installed in it are managed and processed locally.

The system comprises a number of digital recorders, each with its own hard disk, on which the images are stored, and a motion detector. Any movement detected by the cameras in the areas under surveillance is recorded, together with a record of the date, time and place of the recording. All the cameras are in operation 24 hours a day, seven days a week.

Certain sensitive external areas that are not accessible to the public are covered by cameras fitted with infrared beams for night surveillance.

No high-tech or "intelligent" video-surveillance system, sound recording system, talking video-surveillance or covert surveillance system is installed at the Bank. Any derogation, for exceptional reasons and on a limited-duration basis, is subject to obligatory prior notification to the EDPS and/or to the Bank's DPO.

The list of cameras and recorders by site is annexed to the detailed policy and may be consulted on request (see sections 10 and 11).

4.2. Purpose of the surveillance

The Bank uses its video-surveillance system for the sole purposes of security and access control. The video-surveillance system helps control access to the premises and helps to ensure the protection of the infrastructure, staff and visitor safety as well as the protection of the property and information located or stored on the premises. It complements other physical security systems such as the access and physical intrusion control systems. It forms part of the measures adopted to reinforce the more general measures applied for security purposes and helps to prevent, deter and if necessary detect any unauthorised physical access, including to areas placed under security or protection, IT infrastructure or operational information. In addition, video-surveillance helps prevent, detect and investigate the theft of equipment or property belonging to the Bank, its visitors or staff or acts threatening the safety of visitors or staff working on the premises (fires or physical assault, for example).

4.3. Purpose limitation

The system is used solely for the purposes set out above. It is not used to monitor the work of staff or their presence at their place of work. Nor is it used for investigative purposes (other than investigating physical security incidents such as acts of theft or unauthorised access). Any transfers of images to investigatory bodies may take place only in exceptional circumstances, in the context of disciplinary or judicial inquiries, in accordance with the provisions of the general video-surveillance policy.
The use and processing of data for investigative purposes require the prior approval of the DPO and/or the EDPS.

4.4. Ad hoc surveillance activities

Where video-surveillance activities are conducted on an ad hoc basis, a register of such operations is kept by the Security and Services Unit in respect of any data consultation.

4.5. No collection of special categories of data

The video-surveillance systems installed in the Bank's buildings are not intended to capture (by zooming in or deliberate choice of camera angles, for example) or, in general terms, to process images (by indexing them or establishing profiles) that may reveal "special categories of data", namely: racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or data concerning health or sex life[1].

No monitoring of areas likely to reveal, via the images recorded, data relating to these special categories is carried out by the Bank's video-surveillance systems.

[1] See Article 10 of the Regulation.

5. Who has access to the data collected and to whom is this data communicated?

5.1. The staff responsible for internal security and outsourced security guards

Video-surveillance recordings may only be accessed by the official responsible for data processing, i.e. the Head of the Security and Services Unit. The security guards also have access to images as they are filmed during their working hours but may only view them live and have no possibility of carrying out searches or replaying the images. These guards work for an outsourced security firm that is present on site.

5.2. Access rights

The Bank's general video-surveillance policy states clearly and precisely who has access to the filmed images or to the technical architecture of the video-surveillance system, to what end these access rights are created and what is the nature of those rights. That document determines in particular who is authorised to:

- view the images in real time;
- view the recorded images;
- copy;
- download;
- delete;
- export the data
- carry out technical maintenance….

5.3. Staff data protection training

All members of staff holding access rights, including the outsourced security guards, have received data protection training**.** All new members of the security staff are given training when they commence their duties (see point 8.2 of the general policy).

5.4. Confidentiality undertaking of the security staff

On completion of their training, all members of the security staff sign a confidentiality undertaking. This undertaking forms an integral part of the contract of the outsourced firm. These undertakings are included in the Bank's general conditions attached to any outsourcing or consultancy contract.

5.5. Data transfer and communication

Any transfer or communication of data can only be undertaken by the official responsible for data processing, i.e. the Head of the Security and Services Unit, and is subject to prior notification of the Bank's Data Protection Officer (DPO) and/or the European Data Protection Supervisor (EDPS). Any act involving the transfer or communication of data to recipients outside the Security Service is logged and is subject to a rigorous evaluation to assess the need for such act and the compatibility of the intended purpose with that originally pursued, namely security and access control.

These transfers are logged in a register held by the Security and Services Unit.
Management and the staff of the Human Resources Department have no right of access to data.

6. How is collected data protected?

To ensure the security of the video-surveillance system, and especially of personal data, a number of technical and organisational measures have been taken. These measures are set out in detail in the Bank's general video-surveillance policy.

The measures introduced include the following:

- The servers on which the images are stored are located in secure locations, protected by physical security arrangements; fire-protection measures are in place around the IT infrastructure. Lastly, the main IT systems holding the data are covered by enhanced protection measures;
- The access rights given to users entitle them to access only those resources that are absolutely essential for the performance of their duties;
- Only the system administrator, who is specifically designated for this purpose by the official responsible for data processing, is able to grant, modify or cancel a person's access rights. Any grant, modification or cancellation of access rights is governed by the criteria laid down in the general video-surveillance security policy.
- The general video-surveillance security policy includes an up-to-date list of all the persons who have access to the system at any given moment and describes in detail their access rights.

7. How long is the data kept?

The images are kept for a period of no longer than 21 days. After that period, the recordings are systematically erased. If necessary, images that may be used for investigation purposes or as evidence following a security incident may be retained for a longer period. A record of their retention is kept on a rigorous basis and the need for their retention is regularly reviewed.

8. Public information

8.1. A multi-layer approach

Arrangements are made to ensure that the public is kept appropriately and thoroughly informed of our video-surveillance activities. This information is organised according to a multi-layer approach, which combines the following measures:

- the installation on site of information notices to inform the public of the presence of a surveillance system and to provide the essential information concerning data processing;
- the publication of this video-surveillance policy on the intranet and on our websites for the information of those persons who wish to find out more about the video-surveillance activities of our institution;
- the possibility of consulting a paper version of the general video-surveillance policy upon request to the security service. A telephone and a fax number are provided for any person wishing to obtain further information.

Information notices are also placed close to the areas under surveillance, in particular close to the main entrance, the lifts to the car parks and the entrances to the visitors' car parks.

8.2. Individual notice

In addition to these measures, persons identified via the cameras (for example, by the security guards as part of a security investigation) are also informed of this individually as soon as one or more of the following conditions is fulfilled:

- their identity is mentioned in a data file;
- the video recording is used against them;
- it is retained beyond the normal retention period;
- it is transferred outside the security service;
- the identity of the person concerned is communicated to recipients outside the security service.

The sending of these notifications may be delayed on a temporary basis, for example when more time is needed to prevent, investigate, detect or prosecute criminal offences[2]. The DPO (Data Protection Officer) is consulted on a systematic and immediate basis in respect of all cases of this type in order to guarantee that the rights of the person concerned are respected.

9. Public access to data

Members of the public are entitled to have access to data of a personal nature concerning them held by the Bank in order to have those data rectified or erased.

The arrangements for access to such data for any rectification, blockage or erasure must be coordinated with:

- **The Head of the Security and Services Unit, Person responsible for data processing**
  100 boulevard Konrad Adenauer
  L-2950 Luxembourg
  Tel.: 4379-1

This official may also be contacted for any question relating to the processing of personal data.

[2] Other exceptions listed in Article 20 of the Regulation may also apply in exceptional circumstances.

10. 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 (EC) No 45/2001 have been infringed as a result of the processing of their personal data by the Bank. Before initiating that procedure, we would advise any person wishing to invoke that right to contact:

- **The Head of the Security and Services Unit, Person responsible for data processing**
  100 boulevard Konrad Adenauer
  L-2950 Luxembourg
  Tel : 4379-1

- **The Data Protection Officer (DPO) of the Bank**
  100 boulevard Konrad Adenauer
  L-2950 Luxembourg
  Tel : 4379-1

In accordance with Article 14 of the Regulation, any person affected has the right to have data rectified if the data relating to that person is incorrect by applying to the Head of the Security and Services Unit. After verification of the data, the Head of the Security and Services Unit will make the appropriate changes within fifteen days of the request for rectification.

Where the request is for erasure, the DPO will be consulted by the Head of the Security and Services Unit. Upon receipt of the opinion of the DPO or, where appropriate, of the EDPS confirming the need for erasure of the data, the Head of the Security and Services Unit will undertake such erasure.

European Investment Bank Group

Contacts

For general information:

European Investment Bank Group

European Investment Bank
98-100, boulevard Konrad Adenauer
L-2950 Luxembourg
(+352) 43 79 - 1
(+352) 43 77 04
www.eib.org

EUROPEAN INVESTMENT FUND

EIF headquarters
96, boulevard Konrad Adenauer
L-2968 Luxembourg
(+352) 24 85 1
(+352) 24 85 81301
info@eif.org