EBA xxxx numbering

DD Month YYYY

Insert SC/group acronym/EBA Staff

EBA Regular Use

Video surveillance policy

1. Introduction and purpose

For the safety and security of its building, assets, staff and visitors, the European Banking Authority operates a video-surveillance system. This video-surveillance policy, along with its annexes, describes the Agency's video-surveillance system and the safeguards that the Agency takes to protect the personal data, privacy and other fundamental rights and legitimate interests of those caught on camera.

The Agency has produced this Policy in line with Video-Surveillance Guidelines issued by the European Data Protection Supervisor (EDPS) in 2017[1], from here after referred to as "Guidelines", and the provision of Regulation (EU) 2018/1725EU Data Protection Regulation (EUDPR) applicable to EU institutions and bodies.

2. Scope

The scope of this policy includes:

- Prevention and detection of crime and misconduct;
- Investigation of criminal offences and misconduct;
- Investigation of unauthorised, violent or concealed access to the Agency's premises;
- Investigation of unauthorised access to restricted areas within the Agency;
- Monitoring evacuation procedures to ensure security of staff, visitors and contractors;

Excluded from the scope of this policy is monitoring performance of staff members.

3. Definitions

CCTV Closed Circuit Television

DPO Data Protection Officer

[1] THE EDPS VIDEO-SURVEILLANCE GUIDELINES, 2017, Available here

DVD Digital Video Disc

EC European Commission

EDPS European Data Protection Supervisor

Guidelines EDPS Video-surveillance Guidelines

IP Internet Protocol

IT Information technology

OLAF European Anti-fraud Office

4. Policy statement

How do we ensure that our video-surveillance system is designed with privacy and data protection concerns in mind and is compliant with data protection law?

The Agency has installed a number of electronic and physical security measures to protect data. Only qualified personnel have authorised access to video-surveillance data. The Agency's DPO is informed of all personal data security breaches which may occur.

Compliance status

The Agency's premises have been equipped with Video-surveillance system in accordance with Video-Surveillance Guidelines by the European Data Protection supervisor together with the Agency's procedures.

The Agency processes the images in accordance with Regulation (EU) 2018/1725EU Data Protection Regulation (EUDPR) applicable to EU institutions and bodies and the EDPS Guidelines and Recommendations. For matters of public security, the Agency retains video footage for 30 days.

Self-audit and reviews

The system will be subject to a self-audit; these will take place once every two years and each time there is a significant change to the system.

A periodic data protection review will be undertaken by the security services periodically, the next by June 2020. During the periodic reviews the Agency will re-assess that:

- There continues to be a need for the video-surveillance system;
- The system continues to serve its declared purpose; and that;
- Adequate alternatives continue to be unavailable.

Notification of compliance status to the EDPS

Due to the limited scope of the system, it was not necessary to carry out a privacy and data protection impact assessment (Guidelines, Section 3.2) or to submit a prior checking notification to the EDPS (Guidelines, Section 4.3).

Simultaneously with adopting this video-surveillance policy, the Agency notifies the EDPS of the compliance status by sending a copy of the video-surveillance policy and related documents.

Director'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 made by the Executive Director of the Agency after consulting:

- Corporate Services;
- The Agency's Data Protection Officer (DPO);

and after informing the Staff Committee.

During this decision-making process, the Agency:

- 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 purposes described above in section 1 (See Guidelines, Section 5); and
- Addressed the concerns of the DPO and the Staff Committee (See Guidelines, Section 4);

Transparency

The video-surveillance policy is available on EBA's website.

Privacy-friendly technological solutions

Whenever possible the Agency will use the most privacy-friendly settings and technologies.

What areas are under surveillance?

The video-surveillance system consists of a number of fixed cameras strategically located throughout the Agency. The Agency does not routinely monitor any areas under heightened expectations of privacy such as individual offices, leisure areas or toilet facilities (See Guidelines, Section 6.8). The locations of the cameras have been carefully reviewed to ensure that they minimise viewing areas that are not relevant for the intended purposes (Guidelines, Section 6.1).

All other cameras within the premises of the Agency are managed by the landlord of the building, Europlaza, in accordance with the applicable French (FR) data protection legislation.

What personal information does the Agency collect and for what purpose?

Photographic images are collected for the purpose of identification in accordance with the Scope of this policy.

Summary description and detailed technical specifications for the system

The video-surveillance system is an integrated CCVT system. It supports multi-mode recording with individual channels programmed for continuous lapse recording, alarm-triggered event recording and pre-post alarm event recording. All cameras operate 24 hours a day, seven days a week. The image quality in most cases allows identification of those in the camera's area of coverage (See Guidelines, Section 6.4).

Purpose of the surveillance

The Agency uses its video-surveillance system for the sole purpose of security and safety. The video-surveillance system helps control access and helps ensure the security of the building, the safety of the Agency's staff and visitors, as well as property and information located or stored on the premises. It complements the access control system and reception desk personnel, and forms part of the measures taken pursuant to the broader security policies and helps prevent, deter and if necessary, investigate unauthorised physical access to premises, including unauthorised access to secure areas and protected rooms, IT infrastructure, and operational information. In addition, video-surveillance helps prevent, detect and investigate theft of equipment and assets owned by the Agency, visitors, staff and threats to the safety of personnel working at the office.

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. However, the Agency reserves the rights to submit video evidence that has been obtained during an investigation, or may have been recorded during normal operation of the system to substantiate allegations of criminal activity, gross misconduct, or behaviour which puts others at risk. Also the system may be used as an investigative tool or to obtain evidence in internal investigations or in disciplinary procedures, as outlined in the purpose and scope above.

It can also be used in situations when accidents are investigated or health & safety related incidents.

It is only in exceptional circumstances that the images may be transferred to investigatory bodies in the framework of a formal disciplinary or criminal (See Sections 5.7, 5.8 and 10.3 of the Guidelines).

Ad hoc surveillance

Use of ad hoc video-surveillance operations is not foreseen.

Webcams

The Agency has a number of webcams installed in conference and meeting rooms which are managed by the audio visual technicians. Access to the Audio Visual control room is restricted to a limited number of staff members. The Agency does not envisage the use of webcams for video-surveillance.

Categories of data collected

The Agency does not collect any special categories of data (Section 6.7 of the Guidelines). Data are stored for a period of 30 days. Thereafter all images are deleted, unless they have to be retained for the investigation of security incidents.

What is the lawful ground and legal basis of the video-surveillance

The use of the video-surveillance system is necessary for the management and functioning of the Agency and for the purpose described in point 1 and point 2. Therefore, the Agency has a lawful ground for the video-surveillance (See 5.2 of the Guidelines).

Who has access to the information and to whom is it disclosed

The following officers have access to information:

- The Data Protection Officer, Data Controller, Systems Administrator and the Agency's security systems' service provider.

In exceptional circumstances, exclusively in the case of administrative investigations, information may be disclosed to the Appointing Authority and to the persons who are formally appointed as investigators in the framework of administrative inquiries and disciplinary procedures. Information may also be disclosed to national authorities responsible for criminal enforcement (Guidelines Section 10.4). In each case the DPO will be consulted prior to any information being disclosed.

In-house security staff, security guards and security systems' maintenance provider

Recorded and live video footage is accessible to a limited number of Agency's in-house staff and the Agency's security systems' maintenance provider when involved in maintenance of the system.

Access rights

The Agency's security policy for video-surveillance clearly specifies and documents who has access to the video-surveillance footage and/or the technical architecture of the video-surveillance system, for what purpose and what those access rights consist of. In particular, the document specifies who has the right to:

- View the footage real-time;
- View the recorded footage; or
- Copy;
- Download;

- Delete; or
- Alter any footage.

Data protection training

All personnel with access rights are given regularly data protection training.

Training is provided for new member of staff and workshops on data protection compliance issues are offered at least once every two years for all staff with access rights (See Section 8.2 of the Guidelines).

Transfers

All transfers and disclosures outside the security office are documented subject to a rigorous assessment of the necessity of such transfer, the compatibility of the purposes of the transfer with the initial security and access control purpose of the processing (See Section 10 of the Guidelines). A register of retention and transfers will be kept (See Section 10.5 and 7.2 of the Guidelines). The DPO of the Agency is consulted in each case.

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 the framework of an investigation;
- The Commission's Investigation and Disciplinary Office (IDOC) in the framework of a disciplinary investigation, under the rules set forth in Annex IX of the Staff Regulations of Officials of the European Communities; or
- Those appointed to carry out a formal internal investigation or disciplinary procedure within the Agency.

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 general request for data is accommodated.

How does the Agency protect and safeguard the information

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 Agency's Video-surveillance is established in accordance with Section 9 of the EDPS Video-surveillance Guidelines.

The following measures are taken:

- The servers storing the recorded images are located within secure premises and protected by additional physical security measures;
- Network firewalls to protect the logical perimeter of the IT infrastructure; the main computer systems holding the data are security;

- Administrative measures include the obligation of all non-Agency personnel having access to the system (including those maintaining the equipment and the systems) to be individually security cleared;
- Access rights to users are granted only to the systems which are strictly necessary to carry out their roles;
- Only the system administrator specifically appointed by the controller for this purpose is able to grant, alter or annul any access rights of any persons. Any grant, alteration or annulment of access rights is made pursuant to the criteria established in the Security Policy for Video-surveillance.
- The Agency's keeps an up-to-date list of all persons having access to the system at all times and describes their access rights in detail;
- Stringent management of documentation and images which are downloaded to disk;
- Limited access to the Security Office;
- No longer usable media are safely disposed in such a way that remaining data on them are permanently and irreversibly deleted. This is done in accordance with EU Security Standards and industry best practices.

How long does the Agency keep the data

The images are stored for a maximum of 30 days. Thereafter, all images are overwritten. If any image needs 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.

How does the Agency provide information to the public

The Agency provides information to the public about the video surveillance in an effective and comprehensive manner (See Guidelines, Section 11).

To this end, the Agency follows a multi-layer approach, which consists of a combination of the following three methods:

- On-the-spot notices to alert the public to the fact that monitoring takes place and provide them with essential information about the processing;
- The Agency posts the video-surveillance policy on the EBA website.
- This video-surveillance policy is available at reception upon request. A phone number and an email address are provided in the data protection notice for further enquiries. The Agency also has on the spot notices in the reception area.

Specific individual notice

Individuals are given specific individual notice if they are identified on camera (for example, in a security investigation) provided that one or more of the following conditions apply:

- Their identity is noted in any files/records;
- The video recording is used against the individual;

- Kept beyond the regular retention period;
- Transferred outside the security office; or
- If the identity of the individual is disclosed to anyone outside the security office.

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

How can members of the public verify, modify or delete their information

Members of the public have the right to access the personal data that the Agency holds on them and to correct and complete such data. Any request for access, rectification, blocking and/or erasing of personal data should be directed to EBA's Data Protection Officer (DPO), [dpo@eba.europa.eu], [+33 1 86 52 69 37 or +33 1 86 52 70 08]. The DPO may also be contacted in case of any other questions relating to the processing of personal data.

Whenever possible, the security office must respond to an enquiry in substance within 15 calendar days. If this is not possible, the applicant must be 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.

If specifically requested, a viewing of the images may be arranged or the applicant may obtain a copy of the recorded images on a DVD or other media. In case of such a request, the applicants must indicate their identity beyond doubt e.g. they may bring identity cards when they present themselves for the viewing and also designate the date, time, location and circumstances when they were caught on cameras.

They must also provide a recent photograph that would allow them to be identified from the images reviewed.

At this time, the Agency does not charge applicants for requesting a viewing or a copy of their recorded images. However, the Agency 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 applies under Article 20(1) of the Regulation 2018/1725 in a specific case. For example, following a case-by-case evaluation the Agency 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 freedom 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.

Right of recourse

Every individual has the right to have recourse to the European Data Protection Supervisor 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 Agency. Individuals may also try to obtain recourse by contacting:

The Data Protection Officer of the Agency, Tel. [+33 1 86 52 69 37 or +33 1 86 52 70 08 E-mail: dpo@eba.europa.eu

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

The Agency should comply with data access requests even in the absence of the personal data processed in the file. An acknowledgement of receipt shall be sent within five working days of the receipt of the request. However, the Data Controller shall not be required to send an acknowledgement of receipt if a substantial reply to the request is provided within the same time limit of five working days.

If the Agency is unable or has valid grounds to refuse to comply with the request, the Agency is required to give notification of such matters without delay after receipt of this request stating the reasons for its decision.

Related documents

- **Floor maps of the locations of cameras** (not public)
- **Technical specifications for the cameras and for the video-surveillance system as a whole (including any software and hardware)** (not public)
- **Signed Confidentiality undertakings** (not public)
- **Register of retention and transfer** (not public)
- **EDPS Guidelines:** https://edps.europa.eu/sites/edp/files/publication/10-03-17_video-surveillance_guidelines_en.pdf

ANNEX 1 – Template PERSONAL DATA PROTECTION CONFIDENTIALITY UNDERTAKING

EUROPEAN BANKING AUTHORITY

PERSONAL DATA PROTECTION CONFIDENTIALITY UNDERTAKING

I **(insert full name)**

Position/Title _____

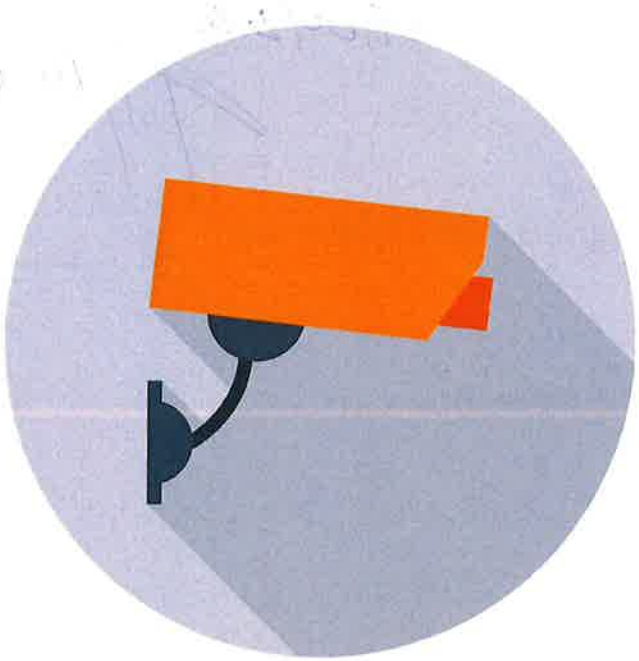
1. undertake to not transfer, show or otherwise disclose the content of any video surveillance footage to anyone except authorised recipients as listed in the EEA Security policy for video-surveillance*;
2. confirm that I have received a copy and read the EBA Video-surveillance policy

Signed: Dated:

The EBA Video-surveillance policy adopted by the EBA Executive Director on XX/YY/ZZZZ were prepared in line with the Guidelines produced by the European Data Protection Supervisor in March 2010, see

ANNEX 2 – On-the-spot data protection notice

EUROPEAN BANKING AUTHORITY



Pour votre sécurité, ce secteur est sous surveillance vidéo de 24 heures. La durée de conservation des enregistrements en vidéosurveillance est de 30 jours. Pour plus d'informations contacter l'Agence à l'adresse security@eba.europa.eu ou dpo@eba.europa.eu, tel: +33 1 86 52 69 37

For your safety and security, this building is under 24 hours video surveillance. The recordings are retained for 30 days. For further information, please contact the Agency's at security@eba.europa.eu or dpo@eba.europa.eu , tel: +33 1 86 52 69 37

Entry into force

This policy enters into force on 28 February 2020.

Date, Signed 27/02/2020
Razvan Gavril, Security Expert

Date, Signed 02/03/2020
Katerina Karypidou, Head of Corporate Support Unit

Date, Signed 2.3.20
Peter Mihalik, Operations Director