eu-LISA Video-surveillance Policy

PUBLIC

Contents

1. Introduction

The present policy (hereinafter "Video-surveillance Policy" or "Policy") defines the purpose, the appropriate use, the responsibilities and the main aspects of the video-surveillance equipment referred to hereafter as closed circuit TV CCTV[1] installed on the premises of the Agency. The need for the CCTV was assessed by the eu-LISA Security Unit, and aims at protecting the Agency from potential damages resulting from an unauthorized entry or providing evidence in the occurrence of such incidents.

2. Purpose and scope of the Agency's Video-surveillance Policy

For the safety and security of its buildings, assets, staff and visitors, our Agency operates a video-surveillance system on both sites in Tallinn, Estonia and in Strasbourg, France and in the premises of the Liaison Office in Brussels (hereinafter "LO"). The scope of this Policy is restricted to the video-surveillance operated by eu-LISA only, where eu-LISA is the controller of the data.

This Video-surveillance Policy, describes the Agency's video-surveillance system, the principles for its use and the safeguards that the Agency implements to protect the personal data, privacy and other fundamental rights and legitimate interests of those persons who are caught on the cameras.

The policy defines the roles and responsibilities with regards to the implementation and use of the video-surveillance system and the processing of the personal data collected in relation to it.

The legal basis for the Policy derives from the following documents:

- Video-Surveillance Guidelines by the European Data Protection Supervisor (hereinafter "EDPS Guidelines") of 2010[2],
- The Regulation No 1077/2011 of the European Parliament and the Council of 25 October 2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (hereinafter as "Establishing Regulation"),
- The Decision of the Management Board on Security Rules in eu-LISA.

3. Privacy-Considerate System Design

3.1. Revision of the existing system

A video-surveillance system had already been operating in the Agency's premises before the issuance of the EDPS Guidelines. The procedures that were in operation, however, have been revised in order to now comply with the recommendations set forth in the EDPS Guidelines.

3.2. Compliance status

The Agency processes the CCTV images in accordance with both the EDPS Guidelines and Regulation

[1] CCTV is herein the term used for video-surveillance, despite the technology used.
[2] EDPS Video-surveillance guidelines available at https://edps.europa.eu/sites/edp/files/publication/10-03-17_video-surveillance_guidelines_en.pdf

(EC) No 45/2001 on the protection of personal data by the Community institutions and bodies.

3.3. Self-audit

The system was subject to an assessment by the eu-LISA's Data Protection Officer (hereinafter "DPO") in order to align compliance of the processing of video-surveillance with the EDPS Guidelines.

3.4. Notification of compliance status to the EDPS

After taking into consideration the limited scope of the system, eu-LISA's DPO concluded that it was not necessary to carry out a formal impact assessment or to submit a prior checking notification to the EDPS.

Simultaneously with the adoption of this Video-surveillance Policy, the Agency will send a copy of it to the EDPS to notify its compliance status.

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

The competent data protection authority in Estonia (the Estonian Data Protection Inspectorate) was informed in July 2015.Their concerns and recommendations were taken into account.

The data protection authority in France (Commission Nationale Informatique et des Libertés or "CNIL") was not informed but the explicit recommendations found on their website were taken into account at that time.

The recommendations issued by the Estonian and French national data protection authorities were respected and the adequate privacy notice is available on the spot at the entrance of both French and Estonian office locations and thus in English, Estonian and French.

3.6. Transparency

This public version of the Video-surveillance Policy may contain summarised information with respect to particular topics or annexes. When this is the case, it is always clearly stated. Information is only omitted from the public version when the preservation of confidentiality is absolutely necessary for compelling reasons (e.g. for security reasons, to preserve the confidentiality of commercially sensitive information or to protect the privacy of individuals).

3.7. Periodic reviews of this Policy

A periodic data protection review will be undertaken by the Security Unit with the DPO once a year.

On the occasion of the annual periodic review, the DPO, together with the Head of Security, will re-assess:

- the continuous need for the video-surveillance system,
- if the system is continuing to serve its declared purpose,
- the possibility to replace elements of the video surveillance system with alternative and equivalent measures.

The periodic reviews will also cover all other issues noted in the former reviews, in particular, whether the Agency's Video-Surveillance Policy continues to comply with the Regulation and the Guidelines (adequacy audit), and whether it is followed in practice (compliance audit).

3.8. Principles for privacy-friendly technological solutions

The Agency shall implement privacy-friendly technological solutions, which include but are not limited to the following principles:

- Blockage of areas where the cameras can be intrusive for the work of the staff or any post-holder, by masking or scrambling images to help eliminate irrelevant areas to the surveillance target;
- Limitation of the view on public and or recreational areas, both internal and external to the premises;
- Blockage of private areas that exterior cameras can visualize, including surrounding private residential areas (eg. by "pixelation" of the private areas included in the video streaming);
- That the surveillance system does not record videos of areas where post-holders work or, if this measure is considered necessary due to the sensitivity of the area, that the recording is only effective outside of working hours;
- The access to the recorded data is password protected and is available only to the specific designated people by the Security Unit team;
- The access to the areas (Security guard rooms) where the video surveillance streaming are processed (Security guards rooms) is restricted to the designated Security personnel; the video streams form the video surveillance systems are not visible from the outside.

3.9. Areas under video surveillance

The system comprises dome and fixed cameras respecting the privacy of the surrounding areas of eu-LISA premises. The Agency does not monitor any areas under heightened expectations of privacy such as individual offices, leisure areas, toilet facilities and others. The location of the cameras shall be regularly reviewed to ensure that they minimise the monitoring of areas that are not relevant for their intended purpose.

Monitoring outside the Agency premises on the territory of Estonia and France is limited to an absolute minimum for the purpose of protecting the Agency, and thus in accordance with national regulation.

4. Personal information collected through the video-surveillance system

4.1. Main technical specifications for the system

The video-surveillance system is a conventional static system. It records digital images and is equipped with motion detection. It records any movement detected by the cameras in the area under surveillance, as well as the corresponding time, date and location. All cameras operate 24 hours a day, seven days a week. The image quality in most cases allows to prevent any intrusion or incident by identification of the movements of persons/vehicles in the camera's area of coverage. The potential use of pan-tilt-and-zoom features for the purpose of following externals, is restricted to the immediate surroundings of the external perimeter. The cameras in use do not record any sound whatsoever. The video-surveillance system may accept inbound alerts/messages from other systems (eg. intrusion detection systems), but will not be connected to external systems with the purpose to

extract video feed or clips. The Agency does not use high-tech or intelligent video-surveillance technology without consulting the DPO, and does not use covert surveillance.

4.2. Purpose of the surveillance

The Agency uses its video-surveillance system for the sole purposes of security, safety and access control. The video-surveillance system helps to control access to the Agency's premises and helps to ensure their security, the safety of Agency personnel and visitors, as well as property and information located or stored on the premises. It complements other physical security systems such as access control systems and physical intrusion control systems. The video-surveillance system is a measure supporting the security policies aiming to 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 to prevent, detect and investigate theft or impairment of equipment or assets owned by the Agency, visitors or staff, and threats to the safety of visitors or personnel working at the office (e.g. fire, physical assault).

4.3. Purpose limitation

The system is not used for any other purpose but the ones specified in section 4.2. The system shall not be used:

- to monitor the work of employees or to monitor their attendance;
- as an investigative tool (other than investigating protective security incidents such as thefts, unauthorised access, attacks).

Only in legally motivated or exceptional circumstances may images from the system be transferred to investigatory bodies in the framework of a formal disciplinary or criminal investigation, as described in Section 5.5 below.

4.4. A*d hoc* surveillance cameras

The Agency uses *ad hoc* surveillance cameras namely equivalent to a video parlophone, which do not record. The cameras are used to facilitate the operational activities of the security guard.

4.5. Webcams

No webcams are operated on the Tallinn and Strasbourg sites, as part of the video surveillance system.

4.6. Special categories of data

The Agency does not collect any special categories of data as defined by the EDPS Surveillance Guidelines.

5. Roles and responsibilities

5.1. General specification

The Executive Director and the Heads of Departments/Units/Sectors shall have a proactive role in communicating this Policy to the staff and to any interested parties.
The Head of Security Unit is responsible for the implementation and enforcement of the Policy.

5.2. Access rights

The data from the video-surveillance system (recorded and live) is only processed by the personnel tasked with the security of the Agency (eu-LISA staff and contracted personnel).
External providers tasked with the maintenance of the video surveillance system might have random and supervised access to the system, for the time necessary to test its functionalities.

5.3. Data protection training

All personnel with access rights, including the outsourced security guards, should receive a data protection training. Training is provided for each new member of the staff and periodic workshops on data protection compliance are carried out at least once every year for all staff with access rights.

5.4. Confidentiality undertakings

Each staff member signs a confidentiality undertaking. This undertaking is also signed by the outsourced company.

5.5. Transfers and disclosures

All transfers and disclosures outside the Security Unit are documented and subject to a rigorous assessment regarding the necessity of such transfer and the compatibility of the purpose of the transfer with the initial security and access control purpose of the processing. The Data Protection Officer of the Agency is consulted in each case.
The following principles shall apply for any transfer or disclosure of data obtained through the video-surveillance system:

I. No access is given to the Agency management or human resources personnel;
II. Local law enforcement authorities may be given access under motivated circumstances, if needed to investigate or prosecute criminal offences;
III. Under exceptional circumstances, access may also be given to:
   - the European Anti-fraud Office ("**OLAF**") in the framework of an investigation carried out by OLAF;
   - 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 carrying out a formal internal investigation or disciplinary procedure within the Agency, provided there is a reasonable expectation that the transfers may help the investigation or prosecution of a sufficiently serious disciplinary offence or a criminal offence.
IV. No requests for data mining will be accommodated.

6. Protection of data

In order to protect the security of the video-surveillance system, including personal data, the Agency shall implement appropriate technical and organisational measures. They are:

- Secure premises, protected by physical security measures hosting the servers storing the

images recorded, network firewalls or physical segregation protecting the logic perimeter of the IT infrastructure, hardened main computer systems holding the data.

- Administrative measures ensuring that all outsourced personnel having access to the system (including those maintaining the equipment and the systems) is always supervised by cleared Agency personnel.
- All staff (external and internal) signs non-disclosure and confidentiality agreements.
- Access rights are granted to users only for the resources which are strictly necessary to carry out their jobs/duties.
- 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 provision, alteration or annulment of access rights is made pursuant to the criteria established in section 5.2. of this Policy.
- The Agency maintains an updated list of all persons having access to the system at all times and describes their access rights in detail. The list shall be created and maintained by the Security Unit.

7. Data Retention

The images obtained through the video surveillance system are retained for a maximum of 30 days. Thereafter, all images are deleted. If any images need to be stored to further investigate or evidence a security incident, they may be retained as necessary. Their retention is rigorously documented and the need for retention is periodically reviewed. The template of the register of retention and transfers is included in Annex 1.

8. Public access to data

8.1. Multi-layer approach

The Agency shall provide information to the public about the video surveillance in an effective and comprehensive manner. To this end, the Agency shall follow a multi-layer approach, which consists of a combination of the following two methods:

- on-the-spot notices to bring to the attention of the public that monitoring is taking place and provide them with essential information about the corresponding processing;
- publication of the Video-surveillance Policy on the Agency intranet and public website, based on the principles underlined in 3.6.

Print-outs of this Video-surveillance Policy shall be made available at the Agency's reception desk and can be obtained upon request from the Security Unit. A phone number and an email address shall be provided for further enquiries. On-the-spot notices adjacent to the areas monitored shall be equally placed. This concerns but is not limited to the main entrance, the elevator entrance in the parking lot and at the entrance of the parking lot.

The Agency's on-the-spot data protection notice is included as Annex 2.

8.2. Specific individual notice

In addition, individuals shall be given individual notice when identified on camera (for example, by

security staff in the process of 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;
- the video recording is kept beyond the regular retention period;
- the video recording is transferred outside the Security Unit;
- if the identity of the individual is disclosed to anyone outside the Security Unit.

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

9. Data subjects rights

Members of the public have the right to access the personal data held by the Agency on them and to correct and/or complete such data. Any request for access, rectification, blocking and/or erasing of personal data should be directed to eu-LISA Head of Security, through the functional mailbox of the Security Unit (eulisa-SECURITY@eulisa.europa.eu).

The Head of Security may also be contacted for any other enquiries related to the processing of personal data.

Whenever possible, the Security Unit 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 of his original enquiry. Even in the most complex of cases, access must be granted, or a final reasoned response must be provided for rejecting the request, and thus within 90 days at the latest from the date of the original enquiry.

The Security Unit must do its best to respond to an enquiry within a reasonable amount of time, especially if the applicant provides an urgent character to his request.

If specifically requested, a viewing of the images may be arranged on-site only. In case of such request, the applicant must establish his identity beyond doubt (e.g. he/she/they should bring an identity card or any other form of legally recognised identity document when attending the viewing) and, whenever possible, also designate the date, time, location and circumstances in which they were caught on cameras. They must also provide a recent photograph of themselves allowing the security staff to identify them from the images being reviewed. In case the number of such access request increases, the Agency reserves the right to charge the applicant with a reasonable fee, proportionate to the time and effort required from the Agency's personnel to fulfil his request.,

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 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 freedoms of others (for example when other people are also present on the images and it is not possible to obtain their consent regarding the disclosure of their personal data or to use image-editing to remedy the latter lack of consent).

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 45/2001 have been infringed as a result of the processing of their personal data by the Agency. Before doing so, the Agency recommends that individuals first try to obtain recourse by contacting:

- the eu-LISA Head of Security (see contact details above), and/or
- the Data Protection Officer of the Agency, through the functional mailbox: dpo@eulisa.europa.eu .

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

11. Enforcement of the policy

The policy shall enter into force on the thirtieth day following its approval and shall be reviewed annually at the initiative of the Security Unit.

The Head of Security is entrusted with the task to enforce the application of the Policy.

Individuals in the Agency, and most notably Agency personnel, can also report observed or suspected violations of this Policy, or other unauthorized activities.

Annex 1: Transfer and disclosure register template

eu-LISA stores the "transfer" and the "disclosure" registers in Tallinn, in the cupboard of the Security Unit. The registers records the information based on the following templates:

Transfer register template

Requesting Authority	Ground for the request	Site	Categories of data	Signature of the authorizing Officer	Date

Retention register template

Requesting Officer	Ground for the request	Site	Categories of data	Extended Retention time	Signature of the Authorizing Officer	Date

Annex 2: On-spot data protection notice

Data Protection notice in Tallinn

Data Protection notice in Strasbourg