European Parliament Video-Surveillance Policy

Adopted by the Deputy Secretary General of the European Parliament
Ms. Francesca R. RATTI

20 April 2013
Updated 28 March 2014

2019 - Ongoing revision

Table of Contents

1. Purpose and scope of the Video-Surveillance Policy

The European Parliament (hereafter: EP) operates a video-surveillance system to prevent, deter and manage, and investigate safety and security incidents as well as for the protection of persons, property and documents against fire, theft, intrusion, assault or any other threat. The video-surveillance system complements other typical security and access control purposes by monitoring specific areas and events. It forms part of the measures to support broader EP security policies.

The data controller for the video-surveillance processing operation is the Director-General for Security and Safety in the EP.

This Video-Surveillance Policy describes the EP video-surveillance system, its purpose and use, and the safeguards that the EP takes to protect the personal data and privacy of those inside the EP and in its immediate surroundings.

The elements of this surveillance policy are valid for the three places of work of the European Parliament, in Luxembourg, Strasbourg and Brussels.

2. 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?

1. Revision of the existing system

A video-surveillance system was already in place within the EP when the Video-Surveillance Guidelines were issued by the European Data Protection Supervisor ("Guidelines") in March 2010. However, EP procedures are regularly under revision to comply with the recommendations set forth in the Guidelines (Section 15), and to improve data protection standards in the EP.

The EDPS Guidelines can be found online:
http://www.edps.europa.eu/EDPSWEB/edps/site/mySite/Guidelines

2. Compliance status

The EP processes the images in accordance with both the Guidelines and Regulation (EC) No 1725/2018 on the protection of personal data by the European institutions and bodies.

3. CCTV System and Data protection self-audit

The EP CCTV system was subjected to a complete camera-by-camera self-audit. For each camera a risk analysis (on security & safety) and an impact assessment (on data protection) was carried out. Based on both analyses and with the objective to minimise the monitoring of areas that are not relevant for the intended purposes, camera locations and viewing angles were modified, removed or confirmed.

In addition, a thorough audit of the current state of play regarding the compliance and adequacy of EP video-surveillance data protection practices with the provisions of the Regulation and the Guidelines has been carried out. Since previously no Video-Surveillance Policy existed the result of this audit is this Policy.

4. Notification of compliance status to the EDPS

When installing or significantly modifying a video-surveillance system, the EP Directorate General for Security and Safety will carry out, with the assistance of the EP-DPO, a formal data protection assessment and, when necessary, will submit a prior checking notification to the EDPS.

This Video-Surveillance Policy and any significant updates are sent to the EDPS. Such exchanges with the EDPS constitute a notification of the EP compliance status on the issue of Video-surveillance.

5. Contacts with relevant data protection authorities in Member States

After adoption, this Video-Surveillance Policy has been sent to relevant authorities in Belgium, France and Luxembourg. Any potential concerns expressed by these authorities will be taken into account in future reviews of this policy.

6. Decision and consultation

The decisions to maintain the video-surveillance system already in place, to verify the existing practices, to identify targeted, specific adjustments to further improve our level of compliance and finally to adopt the safeguards as described in this Video-Surveillance Policy were made by the EP authorities after consulting:

- the EP- Data Protection Officer
- the EDPS

During this decision-making process, the EP:

- demonstrated the need for a video-surveillance system as proposed in this policy;
- made sure that its purpose is legitimate;
- discussed alternatives and concluded that the use 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 in point 1 (above);
- addressed concerns of the consulted organisations.

Through the EP Network of Security Correspondents other stakeholders, including the EP staff committee, will be contacted on this Video Surveillance Policy, and potential comments will be taken into account for further development of this policy.

7. Transparency

The Video-Surveillance Policy has two versions, a version for restricted use and this public version available and posted on our internet and intranet sites.[1]

This public version of the Video-Surveillance Policy may contain summary information with respect to particular topics. 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 sensitive information or to protect the privacy of individuals).

8. Periodic reviews

A periodic data protection review will be undertaken by the Directorate General for Security and Safety every two years. During the periodic reviews it will re-assess that:

[1] http://www.europarl.europa.eu/atyourservice/en/20150201PVL00034/Security-and-access

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

The periodic reviews will also cover other issues addressed in the first audit report, in particular whether our Video-Surveillance Policy continues to comply with the Guidelines (adequacy audit), and whether it is followed in practice (compliance audit).

9. Privacy-friendly technological solutions

When commissioning new equipment for the system and whenever possible the EP will use the best available privacy-friendly technological solutions.

Based on risk analysis and data protection impact assessment, the EP is already implementing and improving privacy-friendly technological and procedural solutions, such as:

- motion detection;
- restricted access to the system;
- risk-based resolution for the cameras (the resolution is as low as possible for the intended security objective).

3. Which areas are under surveillance?

Camera locations and viewing angles are based on a methodological risk analysis and data protection impact assessment, ensuring that cameras point only at the most relevant locations inside and outside the buildings (point 2.3. above).

Cameras are installed to monitor entry and exit points of the buildings (main entrances, emergency and fire exits and the entrance to the parking lot). In addition, there are cameras monitoring several important stairways or connection points and near some high profile areas that require additional security, such as those where large amounts of money are kept, sensitive meeting rooms and restricted access areas.

In principle, we do not monitor any areas of heightened expectations of privacy such as individual offices or leisure areas, except in very rare cases and under strict conditions, as described in section 4.4. Areas with very high expectations of privacy, such as toilet facilities, are never monitored. Monitoring outside our buildings on the territory of Belgium, Luxembourg and France is limited to a minimum perimeter.

4. Which personal information is collected and for what purpose?

1. Technical specifications for the system

The EP video-surveillance system is a conventional system. 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. It records digital images and is equipped with motion detection. It records any movement detected by the cameras in the area under surveillance, together with time, date and location.

We do not use high-tech or intelligent video-surveillance technology, we do not interconnect our system with other systems and we do not use sound recording or "talking CCTV" (Guidelines, 6.12).

2. Purpose of the surveillance

The European Parliament uses its video-surveillance system for the purposes of safety, security and access control. The video-surveillance system helps controlling access to our buildings and ensuring the security and safety of our buildings, of our members, staff and visitors, as well as property and documents located or stored on the premises.

The Video surveillance system helps prevent, deter, manage and, when necessary, investigate safety and security related incidents, possible threats or unauthorised physical access, including unauthorised access to secure premises and protected rooms, IT infrastructure, or operational information.

Regular risk analysis carried out in light of the EP Global Security Concept confirms that video-surveillance helps preventing, detecting and investigating theft of equipment or assets owned by the EP and by Members, Staff, contractors or visitors, as well as threats to the safety inside the buildings.

3. Purpose limitation

The system is not used for any purpose other than those mentioned above. For instance, it is not used to monitor the work of employees or to monitor attendance. Neither is the system used as an investigative tool for purposes other than those instances described above, or in disciplinary procedures unless a physical security incident or criminal behaviour is involved.

It is only in exceptional circumstances that recordings may be transferred to investigatory bodies in the framework of a formal disciplinary or criminal investigation as described in point 6.5 below.

4. Ad hoc and covert surveillance

No ad hoc surveillance operations are foreseen within the framework of the CCTV system. However, in very limited cases the EP may use, with no link whatsoever to the CCTV system and for limited periods of time, stand-alone covert surveillance, only as the latest resource for serious cases putting at risk the safety and security of the Institution. In these cases of severe security infringements, or in case of doubt whether the evidence or allegations support a reasonable suspicion of a sufficiently serious incident, the Parliament's Data Protection Officer will be consulted. In order to minimise the impact on privacy, these cameras are placed only under strict conditions: following an official written request by the person responsible for the area, a risk and impact assessment of placement (guaranteeing that the risk level outweighs the impact on privacy), and prior written authorisation by the Director General for Security and Safety. Maximum time for placement of such cameras is one month, after which the aforementioned procedure must be repeated.

Once placed, such cameras will record only during predefined times and use motion detection. Recorded images will be watched as soon as possible, and at least once per week, only by the EP officials in charge of the investigation. Relevant images are securely stored along with the investigation for up to ten years, while all other images are immediately deleted.

After conclusion of the investigation, people who have been identified on images relevant for the investigation are notified. In case of criminal offences or threats to other parties, data may be transferred to security services of other EU Institutions or to relevant national authorities. Such transfer is subject to a rigorous assessment of the necessity and to prior approval by the Director General for Security and Safety. A data protection form is signed by the receiving party.

The use of covert surveillance has been submitted to the EDPS for prior checking. The prior checking notification and the ensuing EDPS opinion[2] are attached to this policy. In case of future doubt concerning data-protection issues for specific cases, the DPO will be consulted.

5. Webcams

The EP uses no webcams for security or safety purposes.

6. Special categories of data

The EP's Video-surveillance system does not aim at collecting special categories of data, such as racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, or data concerning health or sexual orientation.

The CCTV system monitors the minimum area necessary to ensure the safety and security of the premises. Considering the high-level of security-exposure of the EP premises (the perimeter is easily accessible), the entrances and the perimeter of the European Parliament are all equipped with cameras. The aim of using these cameras is not for capturing or processing special categories of data or targeting any individual, but to be able to prevent, assess and investigate security-related incidents. The operators of these special cameras receive training on data protection and fundamental rights.

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

The use of our video-surveillance system is necessary for the management and functioning of the EP (for safety, security and access control, point 4.2 above), as laid out in the EP Bureau decision of 16 December 2002, and in more general terms in the EP Bureau decisions of 3 May 2004 and 6 July 2011.

This Video-Surveillance Policy, in turn, forms part of the broader implementing rules and is, as such, regularly updated or adapted responding to possible specific threats, political circumstances or technical possibilities.

In light of the above, the EP has a lawful ground and a clear set of procedures for its video-surveillance system.

6. Who has access to the information and to whom is it disclosed?

1. In-house and outsourced security and maintenance staff

The EP outsources part of its video-surveillance operations.

Live video images are accessible to security guards on duty (dispatching) who work for an external security company, based on the need-to-know principle. Outsourced operators have access to recorded footage only when given express approval by the head of the Risk Assessment Unit or Safety and Security Unit.

The CCTV computer system does not allow outsourced operators to extract footage into external media (such as DVD or flash drive). Only EP officials from the Directorate General for Security and Safety are allowed to carry out this type of operation which is at all times duly registered.

The maintenance of the video-surveillance system is also carried out by a contractor, under the supervision of an EP security official.

[2] https://edps.europa.eu/sites/edp/files/publication/13-12-17_video_surveillance_ep_en.pdf

The obligations of both contractors (security and maintenance) with respect to data protection are in writing and in a legally binding manner. They must also provide appropriate training to their staff on data protection.

2. Access rights

The EP's Security Policy for Video-surveillance 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;
- copy;
- download;
- delete;
- alter any footage.

3. Data protection training

All personnel with access rights, including the outsourced security guards and maintenance technicians, are given 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.

4. Confidentiality undertakings

Personnel with access rights, including outsourced personnel carrying out the day-to-day CCTV operations or the maintenance of the system, sign confidentiality undertakings to ensure that they will not transfer, show, or otherwise disclose the content of any video-surveillance footage to anyone except authorised recipients.

5. Transfers, disclosures and registers

Information gathered as a result of processing of personal data, including CCTV images, may be disclosed to the security services of other European institutions or to security, judicial, or law enforcement authorities of EU member states for the purpose of ongoing inquiries or to investigate or prosecute criminal offences. Such transfers are carried out only on request. No regular or routine transfers take place.

All transfers and disclosures outside the Directorate General for Security and Safety are subject to a rigorous assessment of the necessity of such transfer, and duly documented.

No access to the CCTV system is given to management or human resources for purposes other than those described in this Policy.

The need to use recorded footage (point 4.2. above) may involve several Units of the Directorate General, i.e. the Safety and Security Units Brussels, Strasbourg, and Luxembourg, the Dispatching Unit, and the Risk Assessment Unit. Each unit is responsible for compliance with the procedures and data protection safeguards discussed in this Policy as well as with Notifications by the Directorate General to the DPO, and each unit maintains its own registers discussed in this Policy.

7. How do we protect and safeguard the information?

In order to protect the security of the video-surveillance system as a whole, including personal data, a number of technical and organisational measures are being revised and gradually put in place.

These are detailed in a processing-specific Security Policy for the Video-surveillance system. The EP's Security Policy for Video-surveillance was established in accordance with Section 9 of the EDPS Video-surveillance Guidelines.

All the possible technical and physical measures are being taken to ensure the security of the system and the safeguard of data protection, among others:

Personnel (external and internal) are bound by non-disclosure and confidentiality agreements.
Users are granted access right only to those resources which are strictly necessary to carry out their jobs (need-to-know basis).

The EP's Security Policy for Video-Surveillance contains an up-to-date list of all functions/posts having access to the system at all times and describes their access rights

8. How long do we keep the data?

Based on a risk analysis and data protection impact assessment the retention period is individually decided for each camera, with a maximum of 30 days. This prolonged retention period is essential for security investigations, as in many cases complaints are launched a long time after the event, due to presence of users in different places of work.

If any image needs to be stored to further investigate or evidence a security incident, it may be retained for the duration of the investigation and, when relevant, archived along with the investigation for up to ten years. Their retention is rigorously documented.

9. How do we provide information to the public?

1. Multi-layer approach

We provide information to the public (those passing by the EP perimeter and/or those entering into its premises or parking-entrances) about the video-surveillance in an effective and comprehensive manner. To this end, we follow a multi-layer approach, which consists of a combination of the following three methods:

- On-the-spot notices to alert the public (pedestrians, drivers, visitors, staff, etc.) to the fact that monitoring takes place and provide them with essential information about the processing;
- The availability of a summary of this Video-Surveillance Policy at reception desks (annexed to the Notice to visitors);
- The availability of this Video-Surveillance Policy on our intranet and also on our internet sites for those wishing to know more about the video-surveillance practices of our Institution.

An email address is provided for further questions and information on the right to recourse.

2. Specific individual notice

Individuals will also be given individual notice if they were identified on camera (for example, by security staff in a security investigation) provided that one or more of the following conditions also applies:

- their identity is kept in a file
- their identity is kept beyond the regular retention period;
- the video recording is used against the individual;

- the images are transferred outside the DG;
- the identity of the individual is disclosed to anyone outside the DG.

Nevertheless, individual provision of notice may be waived or delayed temporarily as long as considered necessary for security and safety reasons, for example, if this is needed for the prevention, investigation, detection and prosecution of possible criminal offences, terrorist acts or other exceptions under Article 25 of the Regulation.

If such a situation arises and in case of doubt regarding compliance with data protection rights the Directorate General for Security and Safety will seek pertinent advice from the EP - DPO.

10. How can members of the public verify, modify or delete their data?

Members of the public have the right to access the personal data we hold 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:

European Parliament
Directorate General for Security and Safety
Rue Wiertz 60
B-1047 Brussels
E-mail address: SAFE.dataprotection@europarl.europa.eu
Tel: +32 2 28 43727

The Directorate General for Security and Safety may also be contacted in case of any other questions relating to the processing of personal data.

The Directorate General for Security and Safety 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 will be granted or a final reasoned response will be provided rejecting the request within three months at the latest. The services will do their best to respond earlier, especially if the applicant establishes the urgency of the request.

If specifically requested, a viewing of the images may be arranged or the applicant may obtain a copy of the recorded images. In case of such a request, the applicants must indicate their identity beyond doubt (e.g. they should bring identity cards when attending the viewing) and, whenever possible, also designate the date, time, location and circumstances when they were caught on cameras. They must also provide a recent photograph of themselves that allows the security staff to identify them from the images reviewed.

At this time, we do not charge applicants for requesting a viewing or a copy of their recorded images. However, we reserve 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 under Article 25(1) of Regulation 1725/2018 applies in a specific case (see also point 9.2. above). For example, following a case-by-case evaluation we 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 acquire their consent to the disclosure of their personal data or to use image-editing to remedy the lack of consent.

11. Right of recourse

Every individual has the right of recourse to the European Data Protection Supervisor, email address: edps@edps.europa.eu, if they consider that their rights under Regulation 1725/2018 have been infringed as a result of the processing of their personal data by the European Parliament. Before doing so, we recommend that individuals first try to obtain recourse by contacting:

The European Parliament Video Surveillance Data Controller
Directorate General for Security and Safety
E-mail address: SAFE.dataprotection@europarl.europa.eu

and/or

The European Parliament Data Protection Officer
Telephone: +352 4300 23595
E-mail address: data-protection@ep.europa.eu

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