European Parliament Video Protection Policy

Adopted by the
Director-General for Security and Safety of the
European Parliament

Updated January 2022

Table of Contents

1. Scope

The Directorate-General for Security and Safety of the European Parliament (hereinafter 'DG SAFE') uses video protection in order to **monitor specific areas, events, activities, or persons with a visual monitoring system** called closed-circuit television (CCTV).

This video protection policy **describes the European Parliament's video protection system, its purpose and use, and the safeguards** in place to protect the personal rights of data subjects as provided for by Regulation (EU) 2018/1725 on the protection of natural persons with regard to the processing of personal data by the Union institutions (hereinafter 'Regulation (EU) 2018/1725').

2. Purpose limitation

The video protection system provides support when ensuring security and safety as established by the rules governing security and safety in the European Parliament[1].

As such, DG SAFE relies on the video protection system to **prevent, deter or manage possible threats to order and security, including unauthorised physical access** to European Parliament premises or to restricted or sensitive areas, IT infrastructure or information.

DG SAFE may further use CCTV footage **as part of security inquiries and auxiliary investigations** carried out within the scope of its mandate.

Transfers of CCTV recordings only take place in line with the conditions under Section 6.2: 'Disclosures and transfers'.

The video protection system is not used for any other purpose[2].

3. Legal basis

The use of the European Parliament video protection system is governed by the following legal bases:

- European Parliament - Bureau Decision of 15 January 2018 on the rules governing security and safety in the European Parliament) (2018/C 79/04);
- Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation No 45/2001 and Decision No 1247/2002/EC;

[1] European Parliament Bureau Decision of 15 January 2018 on the rules governing security and safety in the European Parliament (2018/C 79/04).
[2] Article 4 of Regulation (EU) 2018/1725.

- European Parliament - Bureau Decision of 17 June 2019 on the implementing rules relating to Regulation (EU) 2018/1725;
- Decision of the Bureau of the European Parliament of 15 April 2013 concerning the rules governing the treatment of confidential information by the European Parliament, OJ C 96, 1.4.2014, p. 1;
- Information Security Policy in the European Parliament of 2 June 2020, Geda (D(2020)14287).

4. Areas under protection

DG SAFE decides on camera locations, viewing angles and areas under video protection, taking full account of the guidelines of the European Data Protection Supervisor[3].

Cameras are positioned following a risk assessment in order to ensure that they are only directed at the most relevant locations, zones and views inside and outside buildings and thus guarantee proper compliance with this policy.

More specifically, cameras are installed to monitor entry and exit points of buildings and in the immediate proximity thereof, including public access zones (such as main entrances, emergency and fire exits, car parks entrances, VIP drop-off points, the Esplanade, etc.). In addition, cameras monitor several important stairways or connection points, as well as high-profile areas that require additional security, such as areas containing valuable assets, confidential and sensitive information, or so-called 'sensitive rooms' and restricted-access areas.

Areas with very high expectations of privacy, such as individual offices or leisure areas, are not monitored.

Monitoring outside Parliament premises is limited to the minimum perimeter necessary to ensure the implementation of the present policy, and done in compliance with the relevant EU and national legislation.

4.1. Ad hoc video protection

In duly justified cases, DG SAFE may use ad hoc video protection for a specific purpose and a limited period of time.

Cameras used for ad hoc video protection are installed following a written request and prior written authorisation from the Director-General of DG SAFE.

Ad hoc video protection may be used for a maximum of one month. Any extension of this period will require the above procedure to be repeated.

Cameras only record during pre-defined times.

[3] The guidelines are available to view at https://edps.europa.eu/sites/edp/files/publication/10-03-17_video-surveillance_guidelines_en.pdf and here at https://edps.europa.eu/data-protection/our-work/publications/guidelines/video-surveillance-follow_en

Images recorded through ad hoc video protection will not be stored, except where designated as relevant for the purposes of a security enquiry, in which case they will be stored with the investigation.

In duly justified cases and after consultation with the Data Protection Officer, ad hoc video protection can be covertly installed.

5. Personal information collected and technical specifications of the system

The European Parliament video protection system is a standard CCTV system. All cameras operate 24 hours a day, seven days a week.

The majority of the cameras only record variations in pixels, meaning that access to proper images is conditional on the detection of a movement by the system. It records any movement detected by the cameras in the area under protection, together with the time, date and location. In that case, the image quality allows for the identification of persons or other details in the footage.

All cameras, whether motion detection or not, are subject to the same strict security measures.

The system does not currently use sound recording CCTV. The European Parliament does not use webcams for video protection.

In accordance with Article 10 of Regulation (EU) 2018/1725, the video protection system is not intended to collect special categories of data.

6. Access to the images and disclosure of the information

6.1 Access rights for agents and system administrators

Only the Director-General of DG SAFE (hereinafter 'the data controller') is authorised to grant, alter or annul access rights.

Access rights are granted to users on a need-to-know basis (those for whom access is strictly necessary for carrying out their tasks) and are limited to the purpose of the present CCTV policy, as well as for technical maintenance of the system.

DG SAFE keeps an internal record of access rights and systematically logs any footage extraction. Footage extraction for technical maintenance takes place without image visualisation.

6.2 Disclosures and transfers

DG SAFE may disclose or transfer CCTV footage to the security services of other European institutions or to security, judicial or law enforcement authorities of an EU Member State.

Such transfers may only occur on request from such parties – there are no regular or routine transfers – and in accordance with the procedure described in this section[4].

Any disclosure or transfer is subject to the approval of the data controller, a rigorous assessment on the necessity of such disclosure or transfer, and the advice of the European Parliament's Legal Service.

In cases involving a Member of Parliament, the formal approval of the President of the European Parliament is required. In cases involving a staff member, the formal approval of the Secretary-General is required.

The European Parliament Data Protection Officer is notified of any such disclosure or transfer.

DG SAFE documents the process in its entirety.

7. Retention period

DG SAFE retains the CCTV footage for one month.

Footage obtained as part of a security investigation is retained for the duration of the undertaking and, when relevant, archived along with the investigation for up to 10 years. DG SAFE rigorously documents such retention.

8. Security measures

The European Parliament uses the best available privacy-friendly technological solutions, in accordance with the principles of 'privacy by design' and 'data minimisation'.

DG SAFE relies on a series of technical and organisational security measures to protect the data contained in the CCTV footage.

As such, the CCTV system is not connected to any other system external to the European Parliament and is only accessible by specifically authorised personnel from DG SAFE. DG SAFE encrypts archived video files during their retention period and scrupulously logs any manipulations of the system.

Furthermore, DG SAFE makes the acquisition of access rights conditional on undergoing mandatory in-house training and confidentiality undertakings.

DG SAFE systematically blurs footage which could lead to the identification of persons not involved in a security enquiry or auxiliary investigation.

[4] DG SAFE does not accommodate requests for 'data mining' or the process of analysing data from different perspectives and summarising it into useful new information.

The necessary arrangements are in place to ensure that the European Parliament video protection system can operate in the event of a power outage to ensure the minimum safety and security conditions.

9. Information to the public

The European Parliament provides information to the public about the video protection system by:

- Issuing on-the-spot notices to alert the public that monitoring takes place and to provide them with essential information about the processing of such monitoring;
- Making a summary of the video protection policy available at reception desks and on the European Parliament website;
- Making the video protection policy available on the European Parliament intranet and internet site.

For all three of these methods, an email address is provided for further questions and information on the respective rights of the data subject.

10. The rights of data subjects

DG SAFE provides individual notice to any person identified on camera if any of the following applies:

Whenever DG SAFE:

- keeps their identity on file;
- keeps their identity beyond the regular retention period;
- uses the footage in proceedings involving the individual;
- discloses or transfers the images outside of DG SAFE.

Members of the public have the right to exercise their personal data protection rights under Regulation (EU) 2018/1725 by addressing any request to the data controller:

The European Parliament Video Protection **Data Controller**
Director-General for Security and Safety
Rue Wiertz 60, B-1047 Brussels
Email address: SAFE.dataprotection@europarl.europa.eu

DG SAFE sends an **acknowledgement of receipt** to the data subject within five working days of receipt of the request[5].

On the substance of the question, DG SAFE **responds to the data subject within 30 calendar days** unless a legitimate reason prevents the data controller from meeting the

[5] This acknowledgement of receipt is not necessary if a substantive reply to the request is provided within the same time limit of five working days. The reply shall be sent to the data subject within the deadlines provided for by Article 14(3) and Article 14(4) of Regulation (EU) 2018/1725.

deadline. The data controller informs the data subject of any possible delays and the reasons thereof.

In order to access their data, data subjects must prove their identity beyond doubt, must indicate – whenever possible – the date, time, location and circumstances of the footage they wish to access, and must provide a recent photograph of themselves to enable DG SAFE to identify them from the images reviewed.

The data controller may refuse to act on a request from a data subject if it is manifestly unfounded or excessive, in particular because of its repetitive character[6]. DG SAFE assesses this on a case-by-case basis. The data controller bears the burden of demonstrating the manifestly unfounded or excessive character of the request.

In the case of a highly complex request, or when the request is likely to result in a risk to the rights and freedoms or other data subjects, the data controller will consult the European Parliament Data Protection Officer.

The European Parliament does not charge applicants for exercising their data protection rights.

The data controller can apply restrictions to the rights granted to data subjects by Regulation (EU) 2018/1725 where **the exercise of such a right would jeopardise the purpose of the security investigation[7].** DG SAFE examines this possibility on a case-by-case basis and, where applicable, duly documents the process and informs the European Parliament Data Protection Officer of any such restriction.

11. The right to lodge a complaint

Every individual has the right to lodge a complaint with the European Data Protection Supervisor (email address: edps@edps.europa.eu) if he or she considers that his or her rights under Regulation (EU) 2018/1725 have been infringed as a result of the processing of their personal data by the European Parliament. DG SAFE recommends that individuals seek to obtain further information before doing so, by contacting:

The European Parliament Video Protection **Data Controller:**
Director-General for Security and Safety
Rue Wiertz 60, B-1047 Brussels
Email address: SAFE.dataprotection@europarl.europa.eu

and/or

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

[6] Article 14 of Regulation (EU) 2018/1725.
[7] Article 25 of Regulation (EU) 2018/1725 and Annex I to the Decision of the Bureau of the European Parliament of 17 June 2019 on the implementing rules relating to Regulation (EU) 2018/1725.

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

12. Consultations and data protection self-audit

The European Parliament operates its video protection system in full compliance with Regulation (EU) 2018/1725.

DG SAFE consulted the European Parliament Data Protection Officer when drafting this policy.

DG SAFE undertakes periodic data protection reviews in order to assess whether:

- it is implementing the video protection policy correctly (compliance audit);
- there continues to be a need for the video protection system;
- the system continues to serve its declared purpose;
- adequate alternatives remain unavailable;
- a data minimisation exercise is implemented regularly.