



Directorate-General for Security and Safety

PROTECTION OF PERSONAL DATA

NOTICE TO VISITORS OF THE EUROPEAN PARLIAMENT PREMISES

The Directorate-General for Security and Safety at the European Parliament (EP) attaches great importance to the right to privacy and protection of personal data. EP Security rules seek to improve transparency and ensure compliance with the legislation on personal data protection (Regulation (EU) No. 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 (EC) No 45/2001 and Decision No 1247/2002/EC).

The Directorate-General for Security and Safety at the EP processes personal data requested from the Institution's Members, staff, contractors, visitors and internal/external partners for the following purposes:

- Granting and controlling access to Parliament's premises.
- Investigating security incidents, evaluating threats, and analysing risks for the EP.

The legal basis governing the operation of the Directorate-General for Security and Safety is the series of decisions of the Bureau of the EP, in particular the Bureau decision of 3 May 2004 (as amended).

Please note that:

(a) Anyone wishing to access Parliament's premises will have to provide their family and first names, date of birth, nationality and type and reference number of an official identity document. The official identity document presented by individual visitors may be scanned to extract such data or to confirm a visitor's identity.

(b) Representatives of interest groups seeking access rights to Parliament will be asked to provide additional personal information in accordance with the rules governing access to EP premises; see also the Notification on Personal Data Processing on the "Accreditation of Representatives of Interest Groups (Lobbyists)"; and the accompanying Privacy statement The Transparency Register of the European Institutions (see http://europa.eu/transparency-register/index_en.htm) indicates those individuals representing organisations and/or self-employed individuals engaged in EU policy-making and policy implementation, to whom the European Parliament has granted access authorisation.

(c) The EP operates a video-surveillance system to prevent, deter, manage, and investigate safety and security incidents. More information on the protection of personal data under the video-surveillance system can be found in the Annex - Note on Video-Surveillance in the European Parliament

(d) Personal data collected from Members, staff, contractors and visitors will not be used for purposes other than those described above. They will not be disclosed to third parties except if necessary for the purposes described above and after prior approval of the Director-General for Security and Safety. Appropriate security measures will be taken to protect the confidentiality of personal data processed and to prevent their misuse by a third party.

(e) Personal data collected is retained for a limited time and is destroyed at the end of the retention period, namely:

- For personal data related to an accreditation request, as outlined at (a) and (b): The validity of the accreditation period plus a maximum of one year (can be extended to two years in specific cases) for purposes of possible security enquiries and risk analyses.
- For personal data (images) related to the CCTV system, please see the Annex.

- For personal data concerning a security incident: Ten years along with the investigation report.

(f) Any individual (Data Subject) has the right to request access to consult and, where applicable, rectify their personal data, as well as other rights including the right to object, on compelling grounds relating to their situation, to the processing of their data and to erasure where duly justified.

(g) The Directorate-General for Security and Safety may restrict the application of the rights under (f), if it could hamper the successful completion of security investigations or create undue operational risks for the EP. The refusal shall then be formally justified to the data subject by the data controller on this basis. The data subject has a right of recourse to the European Data Protection Supervisor.

To exercise your rights or to obtain any further information, you can apply directly to:

Directorate-General for Security and Safety

Data protection coordinator (DPC)

European Parliament

Rue Wiertz 60

B-1047 Brussels

Belgium

E-mail address: SAFE.dataprotection@europarl.europa.eu

Website: <http://www.europarl.europa.eu/at-your-service/en/stay-informed/security-and-access>

Tel: +32 2 28 43727

The European Parliament Data Protection Service

European Parliament

KAD 06A001

L-2929 Luxembourg

E-mail address: data-protection@ep.europa.eu

Website: http://www.europarl.europa.eu/tools/disclaimer/default_en.htm

Tel: +352 4300 23595

The European Data Protection Supervisor

Rue Wiertz, 60

B-1047 Brussels

E-mail address: edps@edps.europa.eu

Website: <http://www.edps.europa.eu/EDPSWEB>

Tel: +32 2 28 31900

Brussels, 29th November 2018

PROTECTION OF PERSONAL DATA

ANNEX - NOTE ON VIDEO-SURVEILLANCE IN THE EUROPEAN PARLIAMENT

This is a summary containing some main issues concerning the European Parliament video-surveillance system and is meant for informational purposes only. The complete Video-Surveillance Policy can be found on the internet at <http://www.europarl.europa.eu/at-your-service/en/stay-informed/security-and-access> or requested by contacting the Directorate-General for Security and Safety, for which the contact details are listed below.

1 - Identity of the data controller

The Data Controller is the Directorate-General for Security and Safety at the European Parliament. Contact details are listed below.

2 - Brief description of the coverage of the video-surveillance system

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, such as main entrances, emergency and fire exits and the entrance to the parking garage, as well as near several important stairways, connection points and some high profile or restricted areas that require additional security. In very rare cases and under very strict conditions, stand-alone cameras may be placed temporarily, not linked to the CCTV system, in the framework of ongoing investigations.

3 - The legal basis of the video-surveillance

European Parliament Bureau decisions of 6 December 2002, 3 May 2004, 6 July 2011, 15 January 2018 and the Video Surveillance Policy approved on 20 April 2013 including subsequent updates.

4 - The data collected and the purpose of the video-surveillance

Data collected: Recorded footage (digital images with time, date and location)

Purpose: 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, and operational information, as well as theft or physical assault.

Purpose limitation: The EP does not monitor any areas under very high expectations of privacy. Monitoring outside our buildings on the territory of Belgium, Luxembourg and France is limited to a minimum perimeter. The system is not used to monitor the work of employees or to monitor attendance. Neither is the system used as an investigative tool or in disciplinary procedures unless a security incident or criminal behaviour is involved.

5 - Who has access to the video-surveillance footage, to whom may the images be disclosed

Who has access to the data: In-house authorised security staff and outsourced authorised security-guards and maintenance personnel.

Disclosures and transfers: Information gathered within the framework of the video-surveillance system 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. All transfers and disclosures outside the Directorate-General for Security and Safety are documented and subject to a rigorous assessment of the necessity of such transfer.

6 - How is the information protected and safeguarded

Technical and physical measures are constantly taken to ensure the security of the system and the safeguarding of data. Access to the video-surveillance footage and/or the technical architecture of the video-surveillance system is restricted to authorised personnel and individual access profiles determine which operations are allowed.

7 - How long are the images kept

Recorded footage is retained for a maximum of 30 days. 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.

8 - How can data subjects verify, modify or delete their information and obtain recourse

The Directorate-General for Security and Safety may be contacted for any questions relating to the video surveillance system and processing of personal data. Members of the public have the right to access their personal data and to correct and complete such data under certain conditions further detailed in the Video-Surveillance Policy. Any request for access, rectification, blocking and/or erasing of personal data should be directed to:

Directorate-General for Security and Safety
Data Controller Video Surveillance EP
Rue Wiertz 60
B-1047 Brussels
Belgium
E-mail address: SAFE.dataprotection@europarl.europa.eu
Tel: +32 2 28 43727

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 (EU) 2018/1725 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 Directorate- General for Security and Safety (contact details above) and/or the European Parliament Data Protection Officer, by telephone: +352 4300 23595 or by e-mail: data-protection@ep.europa.eu.

9 - Hyperlinks related to the EP-Video Surveillance and data protection

The EP Video-Surveillance Policy:
<http://www.europarl.europa.eu/at-your-service/en/stay-informed/security-and-access>

The EDPS Video-surveillance Guidelines:
<http://www.edps.europa.eu/EDPSWEB/edps/site/mySite/Guidelines>