EN

Directorate-General for Security and Safety

PROTECTION OF PERSONAL DATA
NOTICE TO PEOPLE ACCESSING 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. This notice explains how the Directorate-General for Security and Safety handles your information in an open and transparent manner in order to 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 Members of the European Parliament (MEP), staff, contractors, visitors and internal/external partners for the following purposes:

- Granting access to European Parliament's premises;
- Controlling access to European Parliament's premises;
- Investigating security incidents, conducting security inquiries and auxiliary investigations; 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 European Parliament, in particular the Bureau decision of 3 May 2004 (Rules on access badges) (as amended) and EP Bureau Decision on 6 July 2011 (Implementation of the new global security concept) and EP Bureau Decision on 15 January 2018 (Rules governing security and safety in the European Parliament (C79/04)).

Please note that:

(a) Anyone wishing to access Parliament's premises will have to provide the following: his or her family and first names, their date of birth, their nationality as well as the type and reference number of an official identity document and a photo. The official identity document presented by individual visitors may be scanned to extract such data or to confirm a visitor's identity (ID document is not kept nor further processed). Additional personal information regarding vehicles or other assets that will enter Parliament's premises can be collected after a data subject's request.

(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. 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) In order to prevent security incidents, the Directorate-General for Security and Safety may perform security checks on all persons, including Members, goods and assets before they enter and while present on Parliament premises. For that purpose, DG SAFE may collect, while ensuring compliance with the legislation in force in the field of personal data protection, some information about the persons, goods and assets being controlled at the security checks.

(d) The European Parliament operates a video-surveillance (CCTV) system to ensure: the safety, security and access control of its buildings and premises, as well as the safety and security of Members, staff, visitors, properties, archives and documents located or stored on its premises. The system is also intended to prevent (while also deterring) and to manage safety and security incidents. It enables, if necessary, the collection of the necessary elements in order to conduct investigations on incidents and to analyze potential threats. More information on the protection of personal data under the video- surveillance system can be found in the section on Video-Surveillance in the European Parliament.

(e) Personal data collected from Members of the European Parliament (MEP), staff, contractors, visitors and internal/external partners 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.

(f) Personal data collected is retained for a limited time and is destroyed after a reasonable retention period according to the following retention criteria:

- For personal data related to an accreditation request (a) and (b), personal data is retained for the duration of the validity of the accreditation. After this validity, personal data is retained for 2 years for possible investigation needs. Visitor's personal data will be kept for the duration of the visit as well as that of service providers for the duration of their contract. The retention period after these validities will be 1 year (it can also be 2 years in cases of security enquiries and risk analyses). Access logs are kept for 4 months.
- For personal data related to the access controls, personal data can be retained from 1 to 3 years depending on the likelihood of follow-up.
- For personal data (images) related to the CCTV system, please refer to the CCTV Policy.
- For personal data concerning a security incident: ten years along with the investigation report.

(g) Data subjects have the following rights: right to request access to his/her personal data from the controller. He/she shall have the right to obtain, from the controller, the rectification of inaccurate personal data concerning him or her. Data subjects can always contact the European Parliament Data protection service at dataprotection@europarl.europa.eu. The data subjects have the right to lodge a complaint with the European Data Protection Supervisor edps@edps.europa.eu.

(h) The Directorate-General for Security and Safety may restrict the application of the rights under (g), if it could hamper the successful completion of the investigation of security incidents, security enquiries and auxiliary 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.

Please note that certain specific processing activities may be subject to a separate and tailored privacy statement. You can obtain further information at SAFE.dataprotection@europarl.europa.eu and consult the EP Data Protection Register of records at https://www.europarl.europa.eu/data-protect/index.do
Record references / Operation/Process Title:

- 435 - Accréditation - Titres et autorisations d'accès au Parlement européen
- 327 - Contrôles d'accès
- 120 - CCTV

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

The European Parliament Data Protection Service
European Parliament - ADENAUER 14T012 - L-2929 - Luxembourg
E-mail address: data-protection@ep.europa.eu - https://www.europarl.europa.eu/data-protect/index.do
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