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 https://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


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 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 conducting investigations on incidents and to analyze potential threats.

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 management, authorised safety, security and maintenance staff and outsourced authorised security- guards, safety 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:

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

Brussels, 18th November 2019