European Economic and Social Committee

European Committee of the Regions

DATA PROTECTION NOTICE
Video-surveillance policy

Regulation (EU) No 2018/1725 applies to the processing of personal data collected for video-surveillance.

The European Economic and Social Committee (EESC) and the European Committee of the Regions (CoR) use a video-surveillance system to safeguard its buildings, property, staff and visitors. This video-surveillance policy describes the Committees' video-surveillance system and the safeguards that they take in order to protect the personal data, privacy and other fundamental rights and legitimate interests of those individuals whose personal data have been recorded by cameras.

1. Who is responsible for the processing of personal data?

The EESC and the CoR are responsible (as controllers) for the processing of personal data.

The responsible service (as delegated Controller) is the Security Service (secu@eesc.europa.eu).

2. What is the purpose of the processing?

The Committees use their video-surveillance system for the sole purposes of security and access control. The video-surveillance system helps control access to EESC-CoR buildings and helps ensure the security of buildings, the safety of staff and visitors, as well as property and information located or stored on the premises. It complements other physical security systems such as access control systems and physical intrusion control systems. It forms part of the measures to support EESC-CoR broader security policies and helps prevent, deter, and if necessary, investigate unauthorised physical access, including unauthorised access to secure premises and protected rooms, IT infrastructure, or operational information. In addition, video-surveillance helps prevent, detect and investigate theft of equipment or assets owned by the Committees, visitors or staff, and threats to the safety of visitors or personnel working at the office (e.g. fire, physical assault).

The system is not used for any other purpose. For example, it is not used to monitor the work of employees or to monitor attendance. The Committees do not use covert surveillance.

3. What is the legal basis for the processing?

The use of our video-surveillance system is necessary for the management and functioning of the Committees (article 5.1 (a) of the Regulation (EU) No 2018/1725). This forms part of the broader security policies adopted by the Committees, and more specifically the guidelines for the operation of the Security Service. The Committees' videosurveillance policy has been revised in order to comply with the recommendations of the European Data Protection Supervisor (EDPS) Video-Surveillance Guidelines thereafter "Guidelines".

4. What personal data are processed?

Video images digitally recorded.

5. Who are the recipients or categories of recipients of your personal data?

In-house security staff and outsourced security-guards. Recorded video is accessible to in-house security staff only. Live video is also accessible to security guards on duty. These security guards work for an external security company.

Local police may be given access if needed to investigate or prosecute criminal offences. In the course of investigating crimes or offenses or in order to prosecute, images may be transmitted to the Belgian Federal or Local Police. Such requests for disclosure must be reasoned, submitted in writing to the Security Service and must comply with the formal and content requirements imposed by the national legislation in force.

Whenever possible and independently of the obligations imposed at the national level, the Committees will request a judicial warrant, a written request signed by a sufficiently high ranked police officer or a similar formal request. The request should also specify, as accurately as possible, why the video surveillance sequence is required as well the exact place, date and time of the sequence requested.

If the police or another national organisation of a Member State makes a request for access under an official procedure, it must first obtain a waiver of immunity if the sequence in question concerns a member of an Institution of the Union.

Under exceptional circumstances, access may also be given to:

- the European Anti-fraud Office ("OLAF") in the framework of an investigation carried out by OLAF,
- the Commission's Investigation and Disciplinary Office ("IDOC") in the framework of a disciplinary investigation, under the rules set forth in Annex IX of the Staff Regulations of Officials of the European Communities, or
- those carrying out a formal internal investigation or disciplinary procedure within the Institution,

provided that it can be reasonably expected that the transfers may help investigation or prosecution of a sufficiently serious disciplinary offence or a criminal offence.

6. Are your personal data transferred to a third country (non-EU Member State) or international organisation?

Your personal data are not transferred to non-EU Member States or international organisations.

7. How can you exercise your rights?

You have the right to request access to your personal data. Also, you have the right to request rectification or erasure or restriction of the processing of your personal data.

You can direct your queries to (secu@eesc.europa.eu). The query will be dealt with within 15 working days.

You have the right to lodge a complaint to the European Data Protection Supervisor (edps@edps.europa.eu) if you consider that your rights under Regulation EU 2018/1725 have been infringed as a result of the processing of your personal data by the EESC.

8. How long are your personal data kept for?

The images are retained for a maximum of 30 days. Thereafter, all images are automatically erased by the system which overwrites data older than 30 days. In the absence of a security incident, recorded footage of demonstrators is deleted within 48 hours of the end of the protest.

9. Are personal data collected used for automated decision-making, including profiling?

The Committees will not use your personal data to make automated decisions about you. "Automated decisions" are defined as decisions made without human intervention. You have the right to opt out of automated processing at any time and to require that decisions be assessed by a person.

10. Will your personal data be further processed for a purpose other than that for which the data were obtained?

Your personal data will not be further processed for a purpose other than that for which the data were obtained

11. Who can you contact if you have queries or complaints?

If you have any further questions about the processing of your personal data, please contact the unit in charge of the processing of your personal data, (secu@eesc.europa.eu).). You may also contact the EESC Data Protection Officer (data.protection@eesc.europa.eu), the CoR Data Protection Officer (data.protection@cor.europa.eu) and/or the European Data Protection Supervisor (edps@edps.europa.eu) at any time.