European Economic and Social Committee

European Committee of the Regions

Brussels, 4 December 2017

European Committee of the Regions and European Economic and Social Committee video-surveillance policy (Information for the public)

1. Purpose and scope of the Committees' video-surveillance policy

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 has been recorded by cameras.

2. What is the legal basis of video-surveillance

The use of our video-surveillance system is necessary for the management and functioning of the Committees. 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' video-surveillance policy has been revised in order to comply with the recommendations of the European Data Protection Supervisor (EDPS) Video-Surveillance Guidelines (17 March 2010), thereafter "Guidelines".

3. Access to and disclosure of information

3.1 In-house security staff and external security guards

Recorded video is accessible to our in-house security staff only. Live video is also accessible to security guards on duty, including external security staff.

3.2 Data protection training

Training covering data protection compliance issues is provided for each new member of the staff: all personnel with access rights, including the external security guards (see Section 8.2 of the Guidelines). Each staff member, including external security staff, signs a confidentiality undertaking.

4. Protection and safeguarding of data

In order to protect the security of the video-surveillance system, including personal data, a number of technical and organisational measures have been put in place.

Among others, the following measures have been taken:

- Secure premises, protected by physical security measures, host the servers storing the images recorded; network firewalls protect the logic perimeter of the IT infrastructure; and the main computer systems holding the data are security hardened.
- Administrative measures include the obligation of all outsourced personnel having access to the system (including those maintaining the equipment and the systems) to be individually security cleared.
- All staff (external and internal) signed non-disclosure and confidentiality agreements
- Access rights to users are granted only to the data that is strictly necessary to carry out their jobs.
- Only the system administrator specifically appointed by the controller for this purpose is able to grant, alter or annul any access rights of any persons.

5. Informing the public

5.1 Notices at Committee building entrances

Notices posted on site inform the public that video surveillance is in place, and provide essential information on data processing. These notices are posted at all entrances to the Committee's buildings, including the entry to the parking lot.

5.2 Version available at reception

Print-outs of video-surveillance policy are also available at our building reception desks and from our Security Service (secu@eesc.europa.eu) upon request.

5.3 Publication on the Internet

This document is the public version of the video-surveillance policy. It is published on the intranet and the Committees' internet websites.

6. Retention period

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.

7. Verification, modification, blocking and erasure of personal information

Members of the public have the right to access their personal data, to correct it and complete it. Any request for access, rectification, blocking and/or erasing of personal data should be directed to the Security Service (secu@eesc.europa.eu).

At this time, we do not charge applicants for requesting a viewing or a copy of their recorded images. However, we reserve the right to charge a reasonable amount should the number of such access requests increase.

An access request may be refused when an exemption under Article 20(1) of Regulation 45/2001 applies in a specific case.

8. Right of recourse

Every individual has the right of recourse to the European Data Protection Supervisor (edps@edps.europa.eu) if they consider that their rights under Regulation 45/2001 have been infringed as a result of the processing of their personal data by the Committees. Before doing so, we recommend that individuals first try to obtain recourse by contacting:

- the head of the Security Service, secu@eesc.europa.eu
- the relevant Data Protection Officer:
  - the CoR's data protection officer, data.protection@cor.europa.eu
  - the EESC's data protection officer, data.protection@eesc.europa.eu
- staff members may also request a review from their appointing authority under Article 90 of the Staff Regulations