(To be filled in by the DPO)
Register Number: 1466
case number: 2017-0662
Date of submission: 19/6/2017
Legal basis: Notification to the DPO: *Article 25 of the regulation* CE N° 45/2001[1]
Prior checking by the EDPS: A*rticle 27 (5) of the regulation* CE N° 45/2001[2]

NOTIFICATION

INFORMATION TO BE GIVEN[3]

1/ Name and address of the controller (where applicable the deputy data controller)

Philippe Guebels, Head of Security
Directorate for Logistics
Office: JDE0003, Rue Belliard 99-101 – 1040 Bruxelles

2/ Organisational parts of the institution or body entrusted with the processing of personal data
(Unit and directorate of the Data Controller)
Directorate for Logistics (DL), Security Department is responsible for the protection of buildings, property, staff and visitors.

3/ Name and description of the processing
(Please provide a title and describe the action/operation in which personal data is collected/retained and specify the personal data processing operation)
The European Economic and Social Committee (EESC) and the Committee of Regions (CoR) use a video-surveillance system to safeguard its buildings, property, staff and visitors.

The video-surveillance system records digital images in the area under surveillance, together with time, date and location. All cameras operate 24 hours a day, seven days a week.

The video-surveillance system consists of 46 fixed cameras and 33 PTZ (pan-tilt-and-zoom cameras). Of the 79 cameras, 53 are located at entry and exit points of our building, including the main entrance, emergency and fire exits and the entrance to the parking lot. In addition, there is also a camera at the entrance to the stairway in the parking lot.

There are no cameras elsewhere either in the building or outside of it. Areas under heightened expectations of privacy such as individual offices, leisure areas, toilet facilities and others are not monitored.

They can be used by the operators to zoom in on a target or follow individuals around (within the limits of camera's mobility). The image quality in most cases allows identification of those in the camera's area of coverage.

[1] OJ L 8, 12.01.2001.
[2] OJ L 8, 12.01.2001.
[3] Please attach all necessary supporting documents

Monitoring outside EESC-CoR buildings on Belgium territory is limited to an absolute minimum.

4/ Purpose(s) 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, except with the prior authorisation of the Secretary-General in the context of an administrative or disciplinary inquiry after conducting a data protection impact assessment and receiving a positive prior checking opinion from the EDPS. The system is not used as an investigative tool (other than investigating physical security incidents such as thefts or unauthorised access).

5/ Description of the category (ies) of data subject (s)

(Please describe the individuals or group of people whose data is collected and retained)

- EESC and CoR staff
- EESC and CoR members
- Visitors
- External Security company
- Any other person likely to enter the Committees' buildings
- Demonstrators passing in front of the Committees' buildings

6/ Description of the data or categories of data (*including, if applicable, special categories of data (Article 10) and/or origin of data).*

Video images digitally recorded. Due to the location of their buildings and in order to fulfil their security needs, Committees video-surveillance system might record images of protestors that might contain special categories of data, such as political opinions, religious or philosophical beliefs, trade union membership.

7/ Information to be given to data subjects and means of communication (Articles 11 *& 12)*

Information to the public about the video-surveillance is provided in an effective and comprehensive manner:

- on-the-spot notices to alert the public to the fact that monitoring takes place and provide them with essential information about the processing
- a public version of the video-surveillance policy is available on intranet and internet
- print-outs of video-surveillance policy are also available at building reception desks and from security unit (secu@eesc.europa.eu) upon request

Notices are posted at all entrances to the Committee's buildings, including the entry to the parking lot.

8/ Procedures to grant rights of data subjects *(Rights of access, to rectify, to block, to erase, to object)*

Data subjects have the right to access their personal data and to correct and complete such data. Any request for access, rectification, blocking and/or erasing of personal data should be directed to the security service (secu@eesc.europa.eu).

Whenever possible, the security service responds to an enquiry in substance within 15 calendar days. If this is not possible, the applicant is informed of the next steps and the reason for the delay within 15 days. Even in the most complex of cases access must be granted or a final reasoned response must be provided rejecting the request within three months at the latest.

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 contacting EDPS, 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
  - CoR (data.protection@cor.europa.eu)
  - EESC (data.protection@eesc.europa.eu)
- staff members may also request a review from their appointing authority under Article 90 of the Staff Regulation

9/Automated / manual processing operation

Automated. A digital recording and data management system is in place. Special servers are allocated to storing CCTV images.

10/Storage media of data

Each camera signal is continuously recorded by way of a digital video recorder (DVR). Images are digitally recorded on in house hard drives. Special servers are allocated to storing CCTV images (all protected by badge reader).

11/ Legal basis and lawfulness of the pro cessing operation (Article 5)

Article 5a) of the Regulation 45/2001

The use of our video-surveillance system is necessary for the management and functioning of the Committees (for security and access control purpose).

12/ The recipients or categories of recipient to whom the data might be disclosed

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.

No requests for data mining are accommodated. A list of retentions and transfers is kept by the Security Service.

13/ Retention Policy of (categories of) personal data

Footage is retained for a maximum of 30 days, including for special categories of data. Thereafter, all images are automatically erased by the system which overwrites on data older than 30 days.

This retention period is justified by the fact that CoR and EESC members are present on average once a month in the Committees' premises. Therefore, investigating incidents might require accessing records from the previous month. Some images may be stored longer if they are retained as part of an investigation or as evidence of a security incident. Their retention is rigorously documented and the need for retention is periodically reviewed.

13 bis/ Time limit to block and erase the data on justified legitimate request from the data subject)

(Please, specify the time limits for every category, if applicable)

Fifteen working days upon receipt of a request.

14/ Historical, statistical or scientific purposes

(If you store data for longer periods than mentioned above, please specify, if applicable, why the data must be kept under a form which permits identification.)

N/A

15/ Proposed transfers of data to third countries or international organisations

N/A

16/ The processing operation presents specific risk which justifies prior checking *(Please describe):*

YES

The Committees use a video-surveillance system in order to safeguard its buildings, property, staff and visitors. 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.

In this context, the processing of personal data may concern, in particular, suspected offences, offences, infringements and criminal convictions.

AS FORESEEN IN:

– **Article 27.2.(a)**
Processing of data relating to health and to suspected offences, offences, criminal convictions or security measures;

– **Article 27.2.(b)**
Processing operations intended to evaluate personal aspects relating to the data subject;

– **Article 27.2.(c)**
Processing operations allowing linkages not provided for pursuant to national or Community legislation between data processed for different purposes;

– **Article 27.2.(d)**
Processing operations for the purpose of excluding individuals from a right, benefit or contract;

Other (general concept in Article 27.1)

17/ Comments

Obligations of the Controller:

By signing this notification form the Controller guarantees that personal data will be:

- Processed fairly and lawfully
- Collected only for the purpose(s) indicated
- Accurate and kept up to date
- Kept for no longer than necessary

Name and signature of the Controller:

Place and date: