



## EUROPEAN COMMISSION

RESEARCH EXECUTIVE AGENCY  
EUROPEAN RESEARCH COUNCIL EXECUTIVE AGENCY  
EXECUTIVE AGENCY FOR SMALL AND MEDIUM-SIZED ENTERPRISES

### **Data Protection Notice**

#### **Video-Surveillance (CCTV) – Digital and Analogical Storage**

In accordance with the Regulation (EU) No 2018/1725 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 (the Regulation), the Research Executive Agency (REA), the European Research Council Executive Agency (ERCEA) and the Executive Agency for Small and Medium-Sized Enterprises (EASME) (the Agencies) collect your personal information only to the extent necessary to fulfil a precise purpose related to their tasks.

##### **1. WHY DO WE COLLECT YOUR PERSONAL DATA?**

As part of the general management and functioning of the Agencies, the video-surveillance system is used for typical security and access control purposes.

The video-surveillance system serves to efficiently protect the personnel, the goods and the information of the Agencies located in the Covent Garden building complex (buildings COV2 and COVE), the ground floor of the building and its garage as well as the security of the buildings itself<sup>1</sup>. The purpose of the processing of video-surveillance images and recordings is the control of the general access to the building, including certain areas of restricted access.

Video-surveillance is used to prevent (through deterrence), detect and document any security incident that may occur inside the Covent Garden building complex and its perimeter (atrium, parking, etc.) specifically the areas for which the Agencies are responsible. The term ‘security incident’ refers in particular to wrongdoing in the form of intrusion, theft, unauthorised access, break-ins, vandalism, assault, threat, and arson.

The video-surveillance system is not used to monitor employees or other areas such as offices, canteens, kitchenettes, lounges, waiting rooms, toilets, showers or changing rooms.

The video surveillance system may reveal sensitive data (such as racial or ethnic origin), however, the system is exclusively used for typical security and access control purposes and is not meant to capture or process images containing special categories of data.

##### **2. WHO IS RESPONSIBLE FOR THIS PROCESS?**

REA: Head of Department C – “Administration, Finance and Support Services”:  
[REA-LSO@ec.europa.eu](mailto:REA-LSO@ec.europa.eu)

ERCEA: Head of Unit D.2 – “Human Resources”: [ERC-LSO@ec.europa.eu](mailto:ERC-LSO@ec.europa.eu)

EASME: Head of Unit C.2 – “Administration”: [EASME-LSO@ec.europa.eu](mailto:EASME-LSO@ec.europa.eu)

---

<sup>1</sup> This processing operation is limited to the internal cameras installed and operated by the European Commission. Cameras outside the buildings have been deactivated by the owner of the Covent Garden building complex. The agencies have requested to be informed of any future processing activity should the camera system be activated in the future.

### **3. WHAT IS THE LEGAL BASIS TO COLLECT YOUR DATA?**

The processing is necessary for the performance of tasks carried out in the public interest or in the exercise of official authority vested in the Union institution or body (Article 5(1)(a) of the Regulation) and for compliance with a legal obligation to which the controller is subject (Article 5(1)(b) of the Regulation), as established by the following legal acts:

- Regulation 31 (EEC), 11 (EAEC), laying down the Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Economic Community and the European Atomic Energy Community.
- European Commission Video Surveillance Policy managed by the Security Directorate (HR.DS) (Brussels and Luxembourg sites) dated July 2019.
- COMMISSION DECISION (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission.
- COMMISSION DECISION (EU, Euratom) 2015/443 of 13 March 2015 on Security in the Commission.

### **4. WHICH PERSONAL DATA ARE COLLECTED?**

Personal data processed: images.

The cameras record all movements occurring within their viewing angles 24 hours a day, seven days a week. The quality of images, containing facial and body images, can allow the identification of persons in the context of a possible investigation following an infraction.

### **5. WHO WILL HAVE ACCESS TO YOUR PERSONAL DATA?**

The persons with access to the personal data, on a need-to-know basis, are:

Security guards (under contract by DG HR.DS) and staff on duty at the COVE reception and in the Control Room may view live images and they may, in some cases, view shots of a maximum two hours in order to be able to reach on the field any dangerous or infringing situation.

Security staff in the HR.DS Duty Office may view live images and footage recorded less than 24 hours before to be able to take action in case of an incident or infringement.

Only authorised officials in HR.DS and only if justified by a security incident or as part of an inquiry procedure may view images recorded more than 24 hours before. Staff members in HR.DS in charge of maintaining the video surveillance system (Video Management System) may have access to the system components in the context of their professional activities; in some instances, this might include recorded images.

In cases where an investigation is conducted because of a committed offence, it may be deemed necessary to transmit certain data to IDOC or to the competent national authorities responsible for the investigation. Data is transferred only on a portable device, in exchange for an acknowledgement of receipt.

Recorded images may also be transmitted, in compliance with the relevant current legislation and established case law, and on a temporary basis to authorised administrative or judicial authorities, to legislative or supervisory bodies, as well as auditing bodies.

### **6. HOW LONG DO WE KEEP YOUR PERSONAL DATA?**

The recorded images are preserved for a maximum of one month (30 days). This is a reasonable period following a committed offence allowing objective evidence to be available. Legitimate requests to erase images that do not constitute objective evidence in the event of an offence may be handled immediately, unless there are unforeseen technical obstacles. Where a security incident occurs, the above retention period may be extended for the duration of the necessary investigations or the legal and/or administrative proceedings. The process of erasure after the retention period is automatic whereby media is overwritten on a "first-in, first-out" basis.

## **7. WHAT ARE YOUR RIGHTS?**

You are entitled to access the personal data the Data Controllers hold about you and to have your data rectified and completed where necessary.

However, these rights must be strictly limited by the protection of the personal data of third parties who also appear in these images. Therefore, if it is not possible to isolate the images in which the requester alone appears, the individual concerned is informed of the technical reasons making it impossible to provide the images. In such cases, the requester is advised to have the legality of the images concerning him or her checked by the EDPS.

Corrections can only be made by erasing the images in question. This may be done following any legitimate request to erase images that do not constitute objective evidence in the event of an offence, unless there are unforeseen technical obstacles.

To exercise any of these rights or to obtain further information, you should apply to the Data Controllers, who are the responsible of the processing, by sending an e-mail specifying the request to any of the mailboxes indicated below.

## **8. CONTACT INFORMATION**

In case you have any questions about the collection/processing of your personal data, you may contact the data controller who is responsible for this processing activity by using the following email address:

- REA: [REA-LSO@ec.europa.eu](mailto:REA-LSO@ec.europa.eu)
- ERCEA: [ERC-LSO@ec.europa.eu](mailto:ERC-LSO@ec.europa.eu)
- EASME: [EASME-LSO@ec.europa.eu](mailto:EASME-LSO@ec.europa.eu)

The REA, ERCEA and EASME Data Protection Officers are at your disposal for any clarification you may need on your rights under the Regulation at the following e-mail addresses:

- REA: [REA-DATA-PROTECTION-OFFICER@ec.europa.eu](mailto:REA-DATA-PROTECTION-OFFICER@ec.europa.eu)
- ERCEA: [ERC-DATA-PROTECTION@ec.europa.eu](mailto:ERC-DATA-PROTECTION@ec.europa.eu)
- EASME: [EASME-DPO@ec.europa.eu](mailto:EASME-DPO@ec.europa.eu)

You may lodge a complaint to the European Data Protection Supervisor: [EDPS@edps.europa.eu](mailto:EDPS@edps.europa.eu).

[Version July 2020](#)