



EUROPEAN RESEARCH EXECUTIVE AGENCY (REA)  
EUROPEAN RESEARCH COUNCIL EXECUTIVE AGENCY (ERCEA)  
EUROPEAN HEALTH AND DIGITAL EXECUTIVE AGENCY (HADEA)

## **Data Protection Notice**

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

In accordance with the Regulation (EU) 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<sup>1</sup> ('the Regulation'), the European Research Executive Agency ('REA'), the European Research Council Executive Agency (ERCEA) and the European Health and Digital Executive Agency (HADEA) ("the Agencies") collect your personal information only to the extent necessary to fulfil a precise purpose related to our tasks.

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

As part of the general management and functioning of the Agencies, the European Commission (EC) video-surveillance system is used for typical security purposes.

The EC video-surveillance system serves to efficiently protect the staff members, contractors, visitors, and all other persons on its premises, as well as the assets and the information of the Agencies located in the Covent Garden building complex (buildings COV2 and COVE), as well as the security of the buildings itself<sup>2</sup>. The purpose of the processing of video-surveillance (images and recordings) is to control 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, 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.

---

<sup>1</sup> Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 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, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295 of 21.11.2018, p.39).

<sup>2</sup> This processing operation is limited to the internal cameras installed and operated by the European Commission on the floors assigned to the agencies. Cameras on common areas (atrium/ground floor, parking) are operated by the owner of the building complex in compliance with GDPR and Belgian legislation and are part of a separate processing operation. 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.

The recorded images may be further processed to handle investigations following security incidents relating to persons, assets or information and misdemeanours, crimes or other offences. These are covered by other records.

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

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

The processing is done jointly by all the Agencies (acting as joint controllers) hosted in Covent Garden.

For REA, the data controller is REA Head of Department D ‘Coordination and Support Services’ and may be contacted via functional mailbox: [REA-LSO@ec.europa.eu](mailto:REA-LSO@ec.europa.eu).

For ERCEA, the Head of Unit D.2 – “Human Resources” and may be contacted via functional mailbox [ERC-LSO@ec.europa.eu](mailto:ERC-LSO@ec.europa.eu)

For HADEA, the Head of Unit C.3 “Staff, Communication and Support” and may be contacted via functional mailbox [HaDEA-LSO@ec.europa.eu](mailto:HaDEA-LSO@ec.europa.eu)

The main responsibilities of each of the data controllers is to act as primary contact point for their own data subjects wishing to obtain information on video-surveillance and ensure the legality of the filming and of the storage of the images.

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

The processing operations on personal data are carried out under Article 5 (1) of the Regulation (EU) 2018/1725:

- (a) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body; including processing of personal data necessary for the management and functioning of the Union Institutions or bodies [Recital (22) of the Regulation];
- (b) processing is necessary for compliance with a legal obligation to which the controller is subject, which are laid down in Union law and in particular:
  - Articles 8 and 21 of Commission Decision (EU, Euratom) 2015/443 of 13 March 2015 on Security in the Commission;
  - Commission Decision (EU, Euratom) 2016/883 of 31 May 2016 on implementing rules for standard security measures, alert states and management of crisis situations in the Commission;
  - Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission.
  - Article 24 of the Staff Regulations of officials and the Conditions of Employment of other servants of the European Union.

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

The personal data processed in the framework of video-surveillance are images only (no sound, no voice).

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.

These images may incidentally disclose characteristics of the individuals and may allow the identification of ethnic origin, racial identity or health conditions of the individuals, but the processing is not meant to capture or process images containing special categories of personal data.

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

Access is always on a need-to-know basis.

Security guards (under contract with the European Commission Directorate-General for Human Resources and Security - DG HR.DS) may only access live images of the video-surveillance from the Control Room to react immediately to any dangerous situation, and, in some cases, access view shots of a maximum of two hours to be able to reach on the field any dangerous or infringing situation.

Authorised European Commission staff (DG HR.DS) responsible for managing video-surveillance and mandated Security Directorate investigators may also access to data such as live video-surveillance images and recordings of less than 24 hours: they are authorised to retrieve recorded images according to the “need-to-know” principle.

Only authorised officials in DG 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.

In appropriate cases, video-surveillance images may be shared with mandated staff from the Investigation and Disciplinary Office (IDOC) and/or Investigators from the Anti-Fraud Office (OLAF) and the European Public Prosecutor’s Office (EPPO). Such staff abide by statutory confidentiality obligations, and when required, additional confidentiality agreements.

Also, public national authorities may request to have access to these images if such access is necessary for the performance of a task carried out in the public interest or subject to the exercise of their public authority.

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.

Your personal data will be stored on Commission servers located in the EU and will not be transferred to third countries or international organisations.

The processing of your personal data will not include automated decision-making (such as profiling).

## **6. TECHNICAL AND ORGANISATIONAL MEASURES**

Technical and organisational security measures are in place to safeguard the processing of these personal data.

These measures include appropriate actions to address security issues such as data loss, alteration of data or unauthorised access, taking into consideration the risk presented by the processing and the nature of the personal data being processed.

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

We are keeping your personal data for a period of 30 days from the date of recording of the images. This is a reasonable period following a committed offence allowing objective evidence to be available. 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. These are covered by other records.

The process of erasure after the retention period is automatic whereby media is overwritten on a “first-in, first-out” basis.

No further processing is envisaged for historical, statistical, or scientific purposes.

## 8. WHAT ARE YOUR RIGHTS?

You may have access to your personal data and may exercise your right of information / access / rectification / erasure / restriction / data portability / objection / withdrawal of consent by contacting the data controller at: [REA-LSO@ec.europa.eu](mailto:REA-LSO@ec.europa.eu), [ERC-LSO@ec.europa.eu](mailto:ERC-LSO@ec.europa.eu) and [HaDEA-LSO@ec.europa.eu](mailto:HaDEA-LSO@ec.europa.eu).

Your request to exercise one of the above rights will be dealt with within one month. This period may be extended pursuant to Art 14.3 of the Regulation.

Your right to information, access, rectification, erasure, restriction or objection to processing, may be restricted only under certain specific conditions as set out in the applicable Restriction Decision for [REA](#), for [ERCEA and HADEA](#) in accordance with Article 25 of Regulation. Restrictions may also apply due to communication of a personal data breach, or confidentiality of electronic communications.

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.

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.

## 9. 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:ERCEA:ERC-LSO@ec.europa.eu)

[HADEA: HaDEA-LSO@ec.europa.eu](mailto:HADEA:HaDEA-LSO@ec.europa.eu).

You shall have the right of recourse at any time to the competent Data Protection Officer at:

REA Data Protection Officer (DPO): [REA-DATA-PROTECTION-OFFICER@ec.europa.eu](mailto:REA-DATA-PROTECTION-OFFICER@ec.europa.eu)

ERCEA Data Protection Officer: [ERC-DATA-PROTECTION@ec.europa.eu](mailto:ERC-DATA-PROTECTION@ec.europa.eu)

HADEA Data Protection Officer: [HADEA-DPO@ec.europa.eu](mailto:HADEA-DPO@ec.europa.eu)

and the European Data Protection Supervisor: [EDPS@edps.europa.eu](mailto:EDPS@edps.europa.eu)