Data Protection Notice for

Video-Surveillance (CCTV) – Digital and Analogical Storage

The European Health and Digital Executive Agency (HaDEA) processes your personal data[1] in line with Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018[2] on the protection of personal data by the European Union's institutions, bodies and agencies and on the free movement of such data.

What is the purpose(s) of this processing activity?

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 itself3. 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.

---

[1] **Personal data** shall mean any information relating to an identified or identifiable natural person ('data subject'). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

[2] 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 L295/39 of 21.11.2018).

[3] 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.

Who is the data controller?

The data co-controllers of the processing operation are:

- HaDEA: Head of Unit C.3 "Staff, Communication and Support": HADEA-LSO@ec.europa.eu
- REA: Head of Unit D.2 – "People and Workplace": REA-LSO@ec.europa.eu
- ERCEA: Head of Unit D.2 – "Human Resources": ERC-LSO@ec.europa.eu
- EISMEA: Head of Unit C.02 – "People, Workplace and Operational Coordination Support": EASME-LSO@ec.europa.eu

The following **entity process** your personal data on our behalf: European Commission, Directorate-General for Human Resources and Security (DG HR.DS): EC-SECURITY-ACCESS@ec.europa.eu, EC-SECURITY-TECHNIQUE@ec.europa.eu.

Which personal data is collected?

The following of your personal data are collected: images and videos are **mandatory** for the purpose(s) outlined above.

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.

Who has access to the personal data of data subjects and to whom can they be disclosed?

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.

On a need-to-know basis and in compliance with the relevant current legislation, bodies charged with monitoring or inspection tasks in application of EU law (e.g. EC internal audit, Court of Auditors, European Anti-fraud Office (OLAF), the European Ombudsman, the European Data Protection Supervisor, the European Public Prosecutor).

Your personal data **will not be transferred** to third countries or international organisations.

Which is the legal basis for processing your personal 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.

How to withdraw your consent and the consequences of doing this

Not applicable.

How long do we keep your personal data?

Your personal data will be kept for a maximum period of **one** month (30 days) from the records of the images/video on condition that no contentious issues occur. Data will be automatically deleted at the end of this period. 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.

What are your rights regarding your personal data?

You have the right to access your personal data and to request your personal data to be rectified, if the data is inaccurate or incomplete; where applicable, you have the right to request restriction or to object to processing, to request a copy or erasure of your personal data held by the data controller.

Your request to exercise one of the above rights will be dealt with without undue delay and within **one month**.

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:

- HaDEA: HADEA-LSO@ec.europa.eu
- REA: REA-LSO@ec.europa.eu
- ERCEA: ERC-LSO@ec.europa.eu
- EISMEA: EASME-LSO@ec.europa.eu

The HaDEA, REA, ERCEA and EISMEA 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:

- HaDEA: HADEA-DPO@ec.europa.eu
- REA: REA-DATA-PROTECTION-OFFICER@ec.europa.eu
- ERCEA: ERC-DATA-PROTECTION@ec.europa.eu
- EISMEA: EISMEA-DPO@ec.europa.eu

You may lodge a complaint to the European Data Protection Supervisor: EDPS@edps.europa.eu.

Version January 2023