EUROPEAN COMMISSION
RESEARCH EXECUTIVE AGENCY

RECORD OF PERSONAL DATA PROCESSING ACTIVITY

In accordance with Article 31 of 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 (Regulation), individuals whose personal data are processed by the Research Executive Agency (REA or Agency) in any context whatsoever are to be protected with regard to the processing of personal data and the Agency has to keep records of their processing activities.

Record No:
Created on (date):
Last update (date):

NAME OF THE PROCESSING ACTIVITY

Video-Surveillance (CCTV) – Digital and Analogical Storage

GROUND FOR THE RECORD (TICK THE RELEVANT ONE):

☐ *Regularisation of a data processing activity already carried out*
☐ *Record of a new data processing activity prior to its implementation*
☐ *Change of a data processing activity.*
☒ *Migration from notification to record.*

IDENTIFICATION OF THE DATA CONTROLLER

Research Executive Agency (REA):

Head of Department C – "Administration, Finance and Support Services"

European Research Council Executive Agency (ERCEA):

Head of Unit D.2 – "Human Resources"

Executive Agency for Small and Medium-Sized Enterprises (EASME):

Head of Unit C.2 – "Administration"

1. MANDATORY RECORD UNDER ARTICLE 31 OF THE REGULATION

1.1. Name and contact details of controller

REA: Head of Department C – "Administration, Finance and Support Services": REA-LSO@ec.europa.eu

ERCEA: Head of Unit D.2 – "Human Resources": ERC-LSO@ec.europa.eu

EASME: Head of Unit C.2 – "Administration": EASME-LSO@ec.europa.eu

1.2. Name and contact details of the Data Protection Officer (DPO)

- REA: REA-DATA-PROTECTION-OFFICER@ec.europa.eu
- ERCEA: ERC-DATA-PROTECTION@ec.europa.eu
- EASME: EASME-DPO@ec.europa.eu

1.3. Name and contact details of joint controller (where applicable)

For this processing operation the REA, ERCEA and EASME are co-controllers:

- REA: Head of Department C - "Administration, Finance and Support Services": REA-LSO@ec.europa.eu
- ERCEA: Head of Unit D.2 – "Human Resources": ERC-LSO@ec.europa.eu
- EASME: Head of Unit C.2 – "Administration": EASME-LSO@ec.europa.eu

In that respect, the REA, ERCEA and EASME act as **primary contact points** for data subjects wishing to obtain information on video-surveillance and ensure the legality of the filming and of the conservation of the images.

1.4. Name and contact details of processor (where applicable)

European Commission, Directorate-General for Human Resources and Security (DG HR.DS):

EC-SECURITY-ACCESS@ec.europa.eu

EC-SECURITY-TECHNIQUE@ec.europa.eu

1.5. Purpose of the processing

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.[1] The purpose of the processing of video-surveillance

[1] 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

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.

1.6. Legal basis for the processing

- 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.

- Service Level Agreement concerning the collaboration between the Directorate-General for Human Resources and Security of the European Commission and the REA dated 22 January 2018.

- Service Level Agreement concerning the collaboration between DG HR.DS and ERCEA dated 12/02/2018.

- Service Level Agreement concerning the collaboration between DG HR.DS and EASME dated 19/12/2017.

1.7. Categories of data subjects

- Statutory and non-statutory staff working in any of the Agencies located in the Covent Garden building complex;

- Contractors;

- External experts;

---

complex. The agencies have requested to be informed of any future processing activity should the camera system be activated in the future.

- Grant beneficiaries;

- Visitors to the Agencies.

1.8. Categories of personal data

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.

1.9. Retention time (time limit for keeping the 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.

Is any further processing for historical, statistical or scientific purposes envisaged? No

1.10. Recipients of the 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.

1.11. Transfers of personal data to third countries or international organisations

N/A

1.12. High-level description of security measures

Security measures include appropriate access rights and access control. Access to real-time images and electronic recordings is restricted to security personnel of the European Commission.

1.13. Data Protection Notice

A Data Protection Notice (DPN) relevant to this data processing activity is available on the intranet of REA, EASME and ERCEA.

For ERCEA DPN:

http://intranet.ercea.cec.eu.int/services/human-resources/working-environment/Pages/Security%20and%20safety.aspx

For REA DPN:

https://myintracomm.ec.europa.eu/DG/REA/my_daily_work/safety_security_businesscontinuity/safety_security_cove/Pages/default.aspx

For EASME DPN:

http://intranet.easme.cec.eu.int/guides-and-tools/security

The DPN is also available in a paper format upon request at the security desks.