EUROPEAN INNOCATION COUNCIL AND SMEs
EXECUTIVE AGENCY (EISMEA)

EISMEA.C.02 – People, Workplace and Operational Coordination Support

RECORD OF PERSONAL DATA PROCESSING ACTIVITY

*Based on **Article 31 of the Regulation (EU) No 2018/1725**[1] on the protection of natural persons with regards to the processing of personal data by the Union Institutions, bodies, offices and agencies and on the free movement of such data, each responsible EISMEA data controller has to maintain a record of the processing activities under his/her responsibility.*

Record No: R-2019-17-2

Initial approval by Data Controller: *see date of Ares signature*

Previous Notification: DPO-2014-02

Update (s) *(if applicable):* *November 2020*

NAME OF THE PROCESSING ACTIVITY

Video-Surveillance (CCTV) – Digital and Analogical Storage – Covent Garden Building

IDENTIFICATION OF THE DATA CONTROLLER

European Innovation Council and SMEs Executive Agency (EISMEA), Head of Unit C.02 - People, Workplace and Operational Coordination Support – sector C.02.2.

GROUND FOR THIS RECORD (*select relevant ground*)

- □ Record of a new type of processing activity of personal data (before its implementation)
- □ Record of a processing activity of personal data that is already in place (ex-post)
- ☑ Change/Amendment/ Update of an already existing previous record (or previous notification to DPO)

DESCRIPTION OF THE PROCESSING ACTIVITY

The Covent Garden building complex is equipped with surveillance cameras with the aim of protecting not only persons entering the buildings COVE and COV2 occupied by the Executive Agencies (EISMEA, ERCEA, HaDEA and REA - the Agencies) but also their assets and information.

For this purpose, a closed circuit camera system attached to the ceiling of all floors occupied by the Agencies, their access and exit points, the ground floor and the garage has been installed. Images captured by those cameras are monitored in real-time by security officers and recorded/stored, for further use, on secure servers.

[1] 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 295/39 of 21.11.2018).

1. INFORMATION ON THE PROCESSING ACTIVITY
of Video-Surveillance (CCTV) – Digital and Analogical Storage – Covent Garden Building

This processing activity is performed in accordance with **Regulation (EU) No 2018/1725**[2] on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data.

1.1. The Data Controller is:

The Head of Unit C.02 People, Workplace and Operational Coordination Support at the European Innovation Council and SMEs Executive Agency (EISMEA), Place Charles Rogier 16, B-1049 Brussels and and can be contacted at: EISMEA-IRM@ec.europa.eu.

1.2. The following entity(ies) is/are acting as Processor(s) on behalf of the controller on a need-to-know basis:

European Commission, Directorate-General for Human Resources and Security (DG HR.DS): EC-SECURITY-ACCESS@ec.europa.eu; EC-SECURITY-TECHNIQUE@ec.europa.eu

1.3. The legal basis for the processing based on **Article 5(1)** of Regulation (EU) No 2018/1725:

- ✓ **(a)** the 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[3];
- ✓ **(a2**) the processing is necessary for the **management and functioning** of the Union Institutions or bodies (Recital (22) of Regulation (EU) No 2018/1725);
- ✓ **(b)** the processing is necessary for **compliance with a legal obligation** to which the controller is subject, which are:
  - the Service Level Agreement concerning the collaboration between DG HR.DS and the Agency dated 19/12/2017;
  - 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;
- ❒ **(c**) the processing is necessary for the **performance of a contract** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- ❒ **(d)** the data subject has given **consent** to the processing of his or her personal data for one or more specific purposes;
- ❒ **(e**) the processing is necessary in order to protect the **vital interests** of the data subject or of another natural person.

1.4. The purpose(s) of this processing is/are:

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

[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 L 295/39 of 21.11.2018).

[3] *Establishment Act*: Commission Implementing Decision (EU) 2021/173 of 12 February 2021 establishing the European Innovation Council and SMEs Executive Agency (OJ L 50/9 of 15.2.2021).
EISMEA Act of Delegation: Commission Decision C(2021)949 delegating powers to the European Innovation Council and SMEs Executive Agency with a view to the performance of tasks linked to the implementation of Union programmes in the field of Innovative Europe, Single Market and Interregional Innovation Investments comprising, in particular, implementation of appropriations entered in the general budget of the Union.

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. 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 respectively 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.

1.5. The categories of data subjects concerned by this processing are:

- Statutory and non-statutory staff working in any of the Agencies located in the Covent Garden building complex;
- Contractors;
- External experts;
- Grant beneficiaries;
- Visitors to the Agencies.

1.6. The following personal data are collected: 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.

1.7 The recipients to whom the personal data will or might be disclosed 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.

1.8. Personal data will be stored on Agency or Commission servers located in the EU and **will not be transferred to third countries** or **international organisations.**

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

1.10. The following technical and organisational security measures are in place to safeguard the processing of this personal data:

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.

1.11. The personal data concerned **will be kept for a maximum for the following periods:**

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.

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

1.12. Data Subjects are informed on the processing of their personal data via a **data protection notice on their rights :**

- to access their personal data held by a controller;
- to request their personal data held by a controller to be corrected;
- to obtain in some situations erasure of their personal data held by a controller, e.g. when data are held unlawfully (right to be forgotten);
- to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
- **of recourse** at any time to the **EISMEA Data Protection Officer** at EISMEA-DPO@ec.europa.eu and to the **European Data Protection Supervisor** at https://edps.europa.eu.

Request from a data subject to exercise a right will be dealt within **one month**.

The right to information, access, rectification, erasure, restriction or objection to processing, communication of a personal data breach or confidentiality of electronic communications may be restricted only under certain specific conditions as set out in the **applicable Restriction Decision** in accordance with Article 25 of Regulation (EU) 2018/1725.

Any queries concerning the processing of personal data, have to be addressed to the Data Controller indicated above in 1.1. at EISMEA-IRM@ec.europa.eu.

***