Ares(2025)2408322 – 25/03/2025

EUROPEAN INNOVATION COUNCIL AND SMEs EXECUTIVE AGENCY (EISMEA)

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-2019-17-03 **Initial approval by Data Controller**: *see date of Ares signature*

Previous Notification*:* DPO-2014-02 **Update (s)** *(if applicable): March 2025*

NAME OF THE PROCESSING ACTIVITY

Video-Surveillance (CCTV) – Digital and Analogical Storage and Access control to SB34 (Agency's premises)

IDENTIFICATION OF THE DATA CONTROLLER

European Innovation Council and SMEs Executive Agency (EISMEA), Head of Unit C.02, Workplace, IT and Communication

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 SB34 building is equipped with surveillance cameras with the aim of protecting not only persons entering the buildings occupied by the Executive Agencies (EISMEA, EACEA and REA, hereafter '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.

To ensure secure access control and protection of SB34 premises, information and assets, as well as protection of persons present inside SB34 premises, an access control system is in place. This includes technical equipment and information systems and that may include recording of entry to and exit from the SB 34 premises, identity controls on SB34 premises and preventing unauthorised persons from entering SB34 premises.

The processing is done by a range of Information Systems and applications to produce access passes, control building access, monitor variations of noise levels and for video surveillance purposes following security alerts.

[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 – Access control to SB34

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"Workplace, IT & Communication" at the European Innovation Council and SMEs Executive Agency (EISMEA) (the Agency) SB34, B-1049 Brussels and can be contacted at: EISMEA-LSO@ec.europa.eu.

The personal data is processed **jointly with other controllers**, the respective Executive Agencies, hosted in SB34:
- REA Head of Department D 'Coordination and Support Services', who may be contacted via REA-LSO@ec.europa.eu
- EACEA Head of Unit R.1 "People, Workplace and Communication", who may be contacted via EACEA-LSO@ec.europa.eu.

The main responsibilities of each of the data controllers is to act as primary contact point for data subjects wishing to obtain information on access control and video-surveillance and ensure the legality of the filming and of the conservation/storage of the images and ensure the service for video surveillance and access control is part of its security services in the SLA with DG HR.DS[3].

1.2. The following entity(ies) is/are acting as Processor(s):

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

DG HR.DS has the following sub-contractor: 'Protection Unit' - Rue Campagne du Moulin 53/12 – 4470 Saint-Georges-sur-Meuse – Belgium [4].

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[5];
- ✓ **(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:
  - Article 8 (1) and (3) and 21 of Commission Decision (EU, Euratom) 2015/443 of 13 March 2015 on security in the Commission and
  - Commission Decision (EU, Euratom) 2016/883 of 31 May 2016 on implementing rules for standard security measures
  - Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission
  - 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

[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] European Commission Video Surveillance Policy managed by HR.DS
[4] Record of the European Commission (DPR-EC-00654.2)
[5] *EISMEA Establishment Act*: Commission Implementing Decision (EU) 2021/ 173 of 12 February 2021 establishing the European Innovation Council and SMEs Executive Agency.
EISMEA Act of Delegation: Commission Decision C(2021)949 of 12.2.2021 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.

European Atomic Energy Community, and in particular Article 24 SR;
- European Commission Video Surveillance Policy managed by the Security Directorate (HR.DS) (Brussels and Luxembourg sites) dated July 2019;
- the Service Level Agreement concerning the collaboration between DG HR.DS and EISMEA as last updated on14 November 2024.

❒ **(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 as regards the voluntary use of fingerprint data stored on an access badge;

❒ **(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 /are:

A. Video surveillance at SB 34 (CCTV)

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

The video-surveillance system serves to efficiently protect the personnel, the goods and the information of the Agencies located in the EC SB34 building, 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 or outside the SB34 building 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.

This processing operation may also involve the use of recorded images to handle investigations linked to security incidents relating to persons, property or information and misdemeanours, crimes or other offences.

B. Access to SB34 premises

Physical Access Control within the SB34 premises is ensured by the Commission Physical Access Control System (PACS system), implementing the security procedures and policies and producing access rights badges for individuals with a need to access SB34 premises. Additional information is available on the EC Privacy statement and Record for PACS [6].

If the data subject needs access to specific zones protected by biometric devices, fingerprints may be encoded and stored on their personal access pass (badge), which remains with the pass holder. The staff concerned may decide, whether to use this specific access method or opt for an alternative method in these special cases. In order to do so, the data subject will use a Secure Access System (SAS). Alternatively access is granted also with a unique pin code.

Furthermore, if the data subject needs access to the automated car park entrances, his/her car license plate may be video recorded.

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

- Statutory and non-statutory staff of EISMEA or of any other Executive Agencies located in SB34 building or of other European Institutions;
- External persons such as Contractors; External experts; Grant beneficiaries; Visitors to the Agencies including family members of Agency staff.

1.6. The following personal data are collected:

For *the video-surveillance,* the personal data processed are images only (no sound). The cameras record all movements occurring within their viewing angles 24 hours a day, seven days a week. The quality of images,

[6] See EC Privacy statement for PACS and EC Record for PACS DPR-EC-00655.3

containing facial and body images, can allow the identification of persons in the context of a possible investigation following an infraction.
The quality of images, containing facial and body images, may allow the identification of ethnic origin, racial identity or health conditions but the processing is not meant to capture or process images containing special categories of data.

For *the Access control*, the following personal data may be collected: full name, date of birth, photograph, nationality, gender, link with the Agency, current working status, access period, telephone number(s), car license plate number, e-mail, biometric data (fingerprint minutiae if any), identity document number and dates, access rights, specific data related to roles within the Agency (including press, diplomatic representation), access point traversal information – badge number, date, time, direction, alarms and video captures if any. Not all data categories are necessarily processed or retained for each data subject. Data categories processed or recorded are directly related to the kind of link the data subject has with the Agency/ the Commission or the reason for presence.

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 with DG HR.DS) in the Control Room may view live images of the video surveillance to react immediately to any dangerous situation and they may, in some cases, view shots of a maximum two hours to be able to reach on the field any dangerous or infringing situation.
-Security staff in the DG 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 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. Staff members in DG 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 appropriate cases, video surveillance images may be shared with mandated staff from the Investigation and Disciplinary Office (IDOC) and/or Investigators from Anti-Fraud Office (OLAF) and the European Public Prosecutor Office (EPPO). Such staff abide by statutory, and when required, additional confidentiality agreements.
-Recorded images may also be transmitted, in compliance with the relevant applicable 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 for the legitimate performance of their tasks.

1.8. Personal data will be stored on 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.
To ensure secure access control and protection of SB34 premises, information and assets, as well as protection of persons present inside SB34 premises, an access control system is put in place. This includes technical equipment and information systems and that may include recording of entry to and exit from the SB34 premises, identity controls on SB34 premises and preventing unauthorised persons from entering SB34 premises. The processing is done by a range of Information Systems and applications to produce access passes, control building access, monitor variations of noise levels and for *video surveillance* purposes following security alerts.
External cameras cover the immediate surroundings of buildings. Their scopes of vision have been technically limited to avoid scanning areas beyond what is strictly necessary for the immediate security of the Commission's buildings. In some cases, it is not technically possible to exclude sections of public streets/throughways from the scope of certain cameras as they are in close proximity to the monitored

building accesses. In these cases, the potential data subjects are explicitly informed about the presence of cameras (through signs at building entrances). The cameras are visible. DG HR.DS does not use covert Video Surveillance nor does it track movements via location data. However, any section of public streets that cannot be excluded remain marginal, unless there is an imperative need for effective protection of access to buildings occupied by the Institution they represent a certain risk with regard to the protection of its persons, property or information they serve to prevent Commission premises from offences, such as terrorist attacks, intrusions, vandalism or even illegal eavesdropping. In such cases, the Commission notifies the municipal authorities, the police and/or the legal body responsible for the protection of privacy and requests the authorizations provided for by the law of the host country, such as the Belgian law on cameras (Loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance). The cameras are also equipped with digital image masking. Even if they record a street scene, it can be blurred to protect privacy.

Access controls
Biometric data may be used on a voluntary basis as an alternative to the PIN code as a second step multi-factor authentication when entering the SB34 premises following badging in. Biometric data (fingerprint transformed into an algorithm) is stored in a staff member's badge chip on a voluntary basis and in a highly encrypted form. The Commission does not store biometrics in any central database or external system. In order to store the biometric data, a staff member's fingerprint is processed at dedicated station, transformed into an algorithm and saved on their badge.
PIN code and car license plate data is stored on an in-house secure server from the DG HR Security Directorate, with access restricted solely to authorised DG HR Security Directorate personnel.

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.

Fingerprints, that have voluntarily been stored on badges, will remain on the badge for as long as it is being used by the data subject.

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

Your 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-LSO@ec.europa.eu.

***