European Research Council
Executive Agency

Established by the European Commission

RECORD OF PERSONAL DATA PROCESSING

*Art. 31 of the 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 (*henceforth the "Data Protection Regulation"*)*

Record n°	DPO 34 - 2020

In accordance with Article 31 of the data protection regulation, individuals whose personal data are processed by the Executive Agency in any context whatsoever are to be protected with regard to the processing of personal data and the Executive Agency has to keep records of their processing operations.

This record covers two aspects:
1. Mandatory records under Art 31 of the data protection regulation (recommendation: make the header and part 1 publicly available)
2. Compliance check and risk screening (initial; part 2 is internal only to the Agency, not published)

The ground for the record is (tick the relevant one):

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

Video-Surveillance (CCTV) – Digital and Analogical Storage

1	**Last update of this record if applicable**	Digital and analogical Video-Surveillance (CCTV): DPO 53-2012 Ares(2012)1141654 - 28/09/2012
2	**Short description of the processing**	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 (EASME, ERCEA and REA, hereafter the Agencies) but also their assets and information. 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.
Part 1 - Article 31 Record		
3	**Function and contact details of the controller**	Head of Human Resources Unit (ERCEA.D.2) ERC-LSO@ec.europa.eu
4	**Contact details of the Data Protection Officer (DPO)**	ERC-DATA-PROTECTION@ec.europa.eu
5	**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
6	**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
7	**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. 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. **Note**: 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.
8	**Description of the categories of data subjects**	Whose personal data are being processed? ☒ EA staff (Contractual and temporary staff in active position) [Statutory and non-statutory staff working in any of the Agencies located in the Covent Garden building complex]. ☒ Visitors to the EA [Visitors to the Executive Agencies]. ☒ Contractors providing goods or services ☐ Applicants ☐ Relatives of the data subject ☐ Complainants, correspondents and enquirers ☐ Witnesses ☒ Beneficiaries [Grant beneficiaries]. ☒ External experts ☐ Other, please specify:
9	**Description of personal data categories** Indicate **all** the categories of personal data processed and specify which personal data are being processed for each category (between brackets under/next to each category):	*Categories of personal data:* ☐ in the form of personal identification numbers ☒ **concerning the physical characteristics of persons as well as the image, voice or fingerprints** [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]. ☐ concerning the data subject's private sphere ☐ concerning pay, allowances and bank accounts ☐ concerning recruitment and contracts ☐ concerning the data subject's family

		☐ concerning the data subject's career ☐ concerning leave and absences ☐ concerning missions and journeys ☐ concerning social security and pensions ☐ concerning expenses and medical benefits ☐ concerning telephone numbers and communications ☐ concerning names and addresses (including email addresses) ☐ Other :please specify :_____ *Categories of personal data processing likely to present <u>specific risks:</u>* ☐ data relating to suspected offences, offences, criminal convictions or security measures ☐ data being used to evaluate personal aspects of the data subject (ability, efficiency, conduct) *Categories of personal data whose processing is <u>prohibited</u>, with exceptions (art. 10 new Regulation):* ☐ revealing racial or ethnic origin ☐ revealing political opinions ☐ revealing religious or philosophical beliefs ☐ revealing trade-union membership ☐ concerning health ☐ genetic data, biometric data for the purpose of uniquely identifying a natural person ☐ concerning sex life or sexual orientation *Specify any additional data or explanatory information on the data being processed, if any:*
10	**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 archiving purposes in the

		public interest, historical, statistical or scientific purposes envisaged? ☐ yes ☒ no
11	**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.
12	**Are there any transfers of personal data to third countries or international organisations? If so, to which ones and with which safeguards?**	N/A
13	**General description of the technical and organisational 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.
14	**Information to data subjects/Specific Privacy Statement (SPS)**	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.