EUROPEAN EDUCATION AND CULTURE
EXECUTIVE AGENCY (EACEA)

EACEA.R1 - People, Workplace and Communication

RECORD OF PERSONAL DATA PROCESSING

Art. 31 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 "Regulation")

Record nº *13 - 2022*

In accordance with Article 31 of Regulation 2018/1725, individuals whose personal data are processed by the 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 operations.

This record covers two aspects:
1. Mandatory records under Art 31 of the 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 AnalogueStorage	
1	**Last update of this record (where applicable)**
	N/A
2	**Short description of the processing**
	The buildings located at 59 Rue Joseph II (hereinafter: J-59), 70 Rue Joseph II (hereinafter J70), 2 Rue de Spa (hereinafter: SPA-2) and 18 Rue Van Maerlant (hereinafter VM18) (hereinafter referred together as “buildings occupied by EACEA”) are equipped with surveillance cameras with the aim of protecting persons entering the buildings, their assets and information. A camera system is installed in the buildings of the Agency. 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	**Name of the Controller** **Unit(s) and/or function of person acting on behalf of the Controller** The controller is the European Education and Culture Executive Agency (EACEA). For organisational reasons, the role of the data controller is exercised by the Head of Unit R1 ("People, Workplace and Communication") of the EACEA. The controller may be contacted via functional mailbox: EACEA-HR @ec.europa.eu.
4	**Contact details of the Data Protection Officer (DPO)** EACEA-data-protection@ec.europa.eu
5	**Name and contact details of joint controller (where applicable)** N/A
6	**Name and contact details of processor (where applicable)** European Commission, Directorate-General for Human Resources and Security (DG HR): EC-SECURITY-TECHNIQUE@ec.europa.eu
7	**Purpose of the processing** As part of the general management and functioning of the Agency, the video-surveillance system is used for security and access control purposes. The video-surveillance system serves to efficiently protect the personnel, the goods and the information of the Agency located in the buildings occupied by EACEA as well as the security of the buildings itself. The purpose of the processing of video surveillance images and recordings is to prevent, detect and document any security incident that may occur inside the Agency's buildings and its perimeter. This processing operation involves monitoring access to EACEA buildings, including the surroundings at its disposal that are accessible to the public, as well as certain internal areas of the buildings, defined by the sensitivity of the location or the potential risk posed by it or by the repetition of offences or infringements committed there. Under no circumstances shall the monitoring include private premises close to the areas occupied by the EACEA. This processing operation also involves the use of recorded images to handle investigations following security incidents relating to persons, property or information and misdemeanours, crimes, or other offences. The Agency has signed a Service-Level Agreement (SLA) with the Directorate General for Human Resources & Security of the European Commission on 15 December 2017 (Ares (2017)6169601). By virtue of this SLA, HR DS is responsible of the maintenance of the security within the EACEA installations, which includes investigations into security incidents related to staff, assets, and information resources at EACEA.
8	**Description of the categories of data subjects** Whose personal data are being processed? ☒ Agency staff (Contractual and temporary staff in active position) ☒ Visitors to the Agency

	☒ Contractors providing goods or services ☐ Applicants ☒ Relatives of the data subject ☐ Complainants, correspondents and enquirers ☐ Witnesses ☒ Beneficiaries ☒ External experts ☒ Contractors ☒ Other, please specify: **any individual (internal or external to the Agency) passing through the filmed areas**
9	**Description of personal data categories**
	Indicate <u>all</u> the categories of personal data processed and specify which personal data are being processed for each category (between brackets under/next to each category): ***a) 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: images of the data subjects. In the event of reviewing images, any image allowing for the identification of the persons involved in an offence ☐ 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: _____ ***b) 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) ***c) Categories of personal data whose processing is <u>prohibited</u>, with exceptions (art. 10):*** ☐ 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 ***d) 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 30 days. This is a reasonable period following a committed offence allowing objective evidence to be available. A 30-day retention period is considered crucial as an offence may not have been reported immediately. A complaint initiating an investigation is often lodged several days or weeks after the event(s); the HR DS investigators team may have several inquiries ongoing simultaneously and need to prioritise one case over another and return to the latter later. 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 judicial and/or administrative proceedings. **Is any further processing for 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: The persons responsible for managing video surveillance in HR DS and the investigators in competent European Union institutions such as HR DS, IDOC, OLAF and EPPO and competent EACEA's staff. The external contractor of DG HR (Protection Unit). Should an incident indicate potential harm against the European institutions in general, images of the perpetrators may be transferred to the security services of the other European institutions. In the event of an investigation, the data may be given to the competent national authorities responsible for the investigation. Security guards on duty view live images covering the building they are guarding in order to react immediately to any dangerous situation or suspected unlawful act. Guards operating the control room can view live and recorded images from all buildings in order to react to any dangerous situation or suspected unlawful act. When the Internal Inquiries Sector staff carry out investigations within the framework of their own powers, they may view live images and consult and/or use the data contained in the database, to which they have permanent access. Should an offence be committed, or the risk of other similar acts indicate potential harm against the European institutions in general (such as the risk of threats of attack), require the transfer of the images of the perpetrators to the security services of the other European institutions, only the images establishing the objective evidence will be transferred in

	exchange for an acknowledgement of receipt, in compliance with the relevant legal provisions. In cases where an investigation is conducted because of a committed offence, crime, or security incident it may be necessary to transmit certain data bearing the burden of proof to IDOC staff or to the judicial and police authorities responsible for the investigation. This can be done systematically as a matter of urgency following an obvious act of crime or offence, where any delay in the transmission of such information could cause irretrievable damage to the safety of persons, property, or information; or at the written request of the competent magistrate (the most common case). Data is transferred only on a portable device, in exchange for an acknowledgement of receipt.
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**
	The data processing is carried out by European Commission, Directorate-General for Human Resources and Security (DG HR) according to their internal regulations and policies. The data processing is done by 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 / Privacy Statement**
	Individuals with access to the EACEA's internal website may visit the Security and Safety webpage (link). A link to the Privacy Statement is available on this page. The Privacy Statement is also published on EACEA's external website (link).