Ref. Ares(2022)7350747 - 24/10/2022

EUROPEAN EDUCATION AND CULTURE
EXECUTIVE AGENCY (EACEA)

# Video-surveillance (CCTV) – Digital and Analogue Storage

# Privacy Statement

The European Education and Culture Executive Agency ("EACEA") is committed to preserving your privacy. All personal data are dealt with in accordance with Regulation (EU) No 2018/1725 on the protection of personal data by the Union institutions, bodies, offices and agencies[1] ("the data protection regulation").

The following Privacy statement outlines the reasons for the processing of your personal data and the way we collect, manage and use your personal data in relation to the video-surveillance (CCTV) – Digital and Analogue Storage.

## 1. Who is responsible for processing your personal data (data controller)?

The controller is the European Education and Culture Executive Agency, BE-1049 Brussels.
The person designated as being in charge of the processing operation is 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.

## 2. Which personal data are processed?

The personal data processed is images of the data subject captures by the video surveillance system. Cameras film images of the immediate surroundings of the EACEA's buildings, other than private areas, as well as certain rooms or passageways inside these buildings (usual or potential access points or places considered at risk). As a consequence, image recordings of all individuals passing through the filmed areas are processed. In the context of security incidents, those recordings may be reviewed to establish the facts surrounding security incidents or identify an individual.

Individuals who might be filmed are warned locally by the presence of specific pictograms accompanied by a text identifying the responsible department for processing the data and their website.

## 3. For which purpose do we process your data?

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

[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 Text with EEA relevance, OJ L 295, 21.11.2018, p. 39.

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.

By virtue of a Service-Level Agreement (SLA) signed with the Directorate General for Human Resources & Security of the European Commission (DG HR), 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.

## 4. Who has access to your personal data and to whom is it disclosed?

The persons with access to your 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.

## 5. How long do we keep your 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.

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.

## 6. What are your rights concerning your personal data and how can you exercise them?

You can exercise your rights by contacting the Data Controller, or in case of conflict the Data Protection Officer. If necessary, you can also address the European Data Protection Supervisor. Their contact information is given above (section 1) and below (section 8).

Under the provisions of the data protection regulation, you have the right to:

- Request to access the personal data EACEA holds about you;
- Request a rectification of your personal data where necessary;
- Request the erasure of your personal data;
- Request the restriction of the processing of your personal data;
- Request to receive or to have your data transferred to another organization in commonly used machine readable standard format (data portability).

As this processing of your personal data is based on point of Article 5(1)(a) of the data protection regulation, please note that you have the right to object to processing of your personal data on grounds relating to your particular situation under the provisions of Article 23 of the data protection regulation.

Article 25 of the data protection regulation provides that, in matters relating to the operation of EU institutions and bodies, the latter can restrict certain rights of individuals in exceptional circumstances and with the safeguards laid down in that Regulation. Such restrictions are provided for in internal rules adopted by EACEA and published in the Official Journal of the European Union.

Any such restriction will be limited in time, proportionate and respect the essence of the above-mentioned rights. It will be lifted as soon as the circumstances justifying the restriction are no longer applicable. You will receive a more specific data protection notice when this period has passed.

As a general rule you will be informed on the principal reasons for a restriction unless this information would cancel the effect of the restriction as such.

You have the right to make a complaint to the EDPS concerning the scope of the restriction.

## 7. Your right to have recourse in case of conflict on any personal data issue

In case of conflict on any personal data protection issue you can address yourself to the Controller at the above mentioned address and functional mailbox.

You can also contact the Data Protection Officer of EACEA at the following email address: eacea-data-protection@ec.europa.eu.

You may lodge a complaint with the European Data Protection Supervisor at any time: http://www.edps.europa.eu.

## 8. On which legal basis are we processing your personal data?

The processing operation is compliant with the principle of lawfulness and fairness. We process your personal data because:

(a) 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,
(a2) including processing of personal data necessary for the management and functioning of the Union Institutions or bodies [Recital 22].

Under Article 5(1)(a), the applicable legal basis are:

- Commission Implementing Decision 2021/173 establishing the European Education and Culture Executive Agency.
- 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.
- Commission Decision (EU, Euratom) 2015/443 of 13 March 2015 on Security in the Commission, in particular Article 8 (1) and (3):

> *"1. Security of assets shall be ensured by applying appropriate physical and technical measures and corresponding procedures creating a multi-layered system."*
>
> *"3. Physical security shall have the following objectives: […] enabling investigation and inquiry into security incidents including through checks on access and exit control log files, CCTV coverage, telephone call recordings and similar data as referred to in Article 22(2) and other information sources."*


Electronically signed on 24/10/2022 09:10 (UTC+02) in accordance with Article 11 of Commission Decision (EU) 2021/2121