



EUROPEAN RESEARCH EXECUTIVE AGENCY (REA)
EUROPEAN INNOVATION COUNCIL AND SMES EXECUTIVE AGENCY (EISMEA)
EUROPEAN EDUCATION AND CULTURE EXECUTIVE AGENCY (EACEA)

Data Protection Notice

Video-Surveillance at SB34 (CCTV) – Digital and Analogical Storage

and

Access control to the Simon Bolivar 34 (SB34) premises

In accordance with the Regulation (EU) 2018/1725 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 data¹ ('the Regulation'), the European Research Executive Agency (REA), the European Education and Culture Executive Agency (EACEA), and the European Innovation Council and SMEs Executive Agency (EISMEA) ("the Agencies") collect your personal information only to the extent necessary to fulfil a precise purpose related to our tasks.

1. WHY DO WE COLLECT YOUR PERSONAL DATA?

A. Video-Surveillance at SB34 (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, including exit from and presence in the building.

The video-surveillance system serves to efficiently protect any person entering the building, the personnel, the assets and the information of the Agencies located in the European Commission building SB34, the ground floor of the building and its garage as well as the security of the building itself². 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 building and its perimeter (the area just in front of the entrance to the building, 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 recorded images may be further processed to handle investigations following security incidents relating to persons, assets or information and misdemeanours, crimes or other offences. These are covered by other records.

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 of 21.11.2018, p.39).

² This processing operation is related to the internal cameras installed and operated by the European Commission as well as the cameras outside the building. The camera outside the building only records the entrance of the building.

The video-surveillance system is not used to track movements of individuals or monitor other areas such as offices, canteens, kitchenettes, lounges, waiting rooms, toilets, showers or changing rooms nor for time management purpose.

B. Access to SB34 premises

Physical Access Control within the SB34 premises is ensured by the Commission Physical Access Control System (PACS), implementing the security procedures and policies and producing access rights badges for individuals with a need to access the SB34 premises. For staff from the Agencies (badge and fingerprints or PIN code) and for staff from other EU institutions, bodies and other agencies (“EUIBAs”): they will have access by showing their badge. Visitors will need to pre-register in a central web application called V-pass. External contractors are provided with a badge by DG HR.DS. Additional information is available [here](#) (EC PACS privacy statement) and [here](#) (EC PACS Record DPR-EC-00655.3).

If the data subject needs access to the building outside opening hours (weekends or holidays) or to restricted zones protected by biometric devices, the data subject may decide on the specific access method (i.e. fingerprints scanned³ and stored on their personal access badge or PIN code). Entry in these cases is via a Secure Access System (SAS) without the need for a guard to be present.

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

2. WHO IS RESPONSIBLE FOR THIS PROCESS?

The processing is done jointly by all the Agencies (acting as joint controllers) hosted in SB34.

For REA, the data controller is REA Head of Department D ‘Coordination and Support Services’ and may be contacted via functional mailbox: REA-LSO@ec.europa.eu.

For EACEA, the Head of Unit R.1 – “People, Workplace and Communication” and may be contacted via functional mailbox: EACEA-LSO@ec.europa.eu.

For EISMEA, the Head of Unit C.02 – “Workplace, IT and Communication” and may be contacted via functional mailbox: EISMEA-LSO@ec.europa.eu.

The main responsibilities of each of the data controllers is to act as primary contact point for its own data subjects wishing to obtain information on video-surveillance and access control as well as to ensure the legality of the filming and of the storage of the images of the persons entering/being present/exiting the building.

3. WHAT IS THE LEGAL BASIS TO COLLECT YOUR DATA?

The processing operations on personal data are carried out under Article 5 (1) of the Regulation (EU) 2018/1725, relating to the lawfulness of processing:

- (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) processing of personal data necessary for the management and functioning of the Union Institutions or bodies (Recital (22) of the Regulation);

³ Fingerprint data is encrypted as an algorithm and stored only on the badge's chip, without being saved in any central database or external system

- (b) processing is necessary for compliance with a legal obligation to which the controller is subject, which are laid down in Union law and in particular:
 - Articles 8 and 21 of Commission Decision (EU, Euratom) 2015/443 of 13 March 2015 on Security in the Commission;
 - Commission Decision (EU, Euratom) 2016/883 of 31 May 2016 on implementing rules for standard security measures, alert states and management of crisis situations in the Commission;
 - Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission.
 - Article 24 of the Staff Regulations of officials and the Conditions of Employment of other servants of the European Union.
- (d) processing is based on data subjects' consent for one or more specific purposes, namely the voluntary use of fingerprint data stored on his/her access badge if this option to access the building was chosen by the data subjects concerned.

4. WHICH PERSONAL DATA ARE COLLECTED?

For the *video-surveillance*: the personal data processed are images only (no sound, no voice).

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.

These images may incidentally disclose characteristics of the individuals and may allow the identification of ethnic origin, racial identity or health conditions of the individuals, but the processing is not meant to capture or process images containing special categories of personal data.

For the *access control*: the following personal data may be collected from the individuals: first name and last name, date of birth, photograph, nationality, gender, job function, current working status, access period, telephone number(s), car plate number, e-mail, biometric data (fingerprint minutiae (if any), identity document number and dates, access rights, specific data related to roles, 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 or Commission.

5. WHO WILL HAVE ACCESS TO YOUR PERSONAL DATA?

Access is always granted on a need-to-know basis.

For the *video-surveillance*: Security guards (under contract with the European Commission Directorate-General for Human Resources and Security - DG HR.DS -) may only access live images of the video-surveillance from the Control Room to react immediately to any dangerous situation, and, in some cases, access view shots of a maximum of two hours to be able to reach on the field any dangerous or infringing situation.

Authorised European Commission staff (DG HR.DS) responsible for managing video-surveillance and mandated Security Directorate investigators may also have access to this data, such as access to live video-surveillance images and recordings of less than 24 hours: they are authorised to retrieve recorded images according to the “need-to-know” principle.

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.

In appropriate cases, video-surveillance images may be shared with mandated staff from the Investigation and Disciplinary Office (IDOC) and/or Investigators from the Anti-Fraud Office (OLAF), and the European Public Prosecutor Office (EPPO). Such staff abide by statutory confidentiality obligations, and when required, additional confidentiality agreements. Also, public

national authorities may request to have access to these images if such access is necessary for the performance of a task carried out in the public interest or subject to the exercise of their public authority.

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.

For *access control*: The data subject is recipient for the photograph on the data subject's access badge and this photo can be transferred to SYSPER if requested by the data subject.

Within each agency, the Local Security Officers (limited to the staff members in the Agency) is recipient for granting roles in the European Commission Physical Access Control System (PACS) tool, visit requestors and validators (individuals using the systems to request and/or validate requests for visits). Outside the Agency, the recipients are:

- DG HR.DS Staff: System administrators, system operators and security operators; access rights and profiles managers
- Subcontractors of the EC (security guards and Duty Office operators) to ensure security management and monitoring
- External users: end users to manage own request and visitors/visits
- If required by law, PACS data can be transferred to law enforcement bodies and/or judicial authorities.

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

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

6. Technical and organisational measures

Technical and organisational security measures are in place to safeguard the processing of these personal data. More precisely, 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.

These measures include appropriate actions to address security issues such as data loss, alteration of data or unauthorised access, taking into consideration the risk presented by the processing and the nature of the personal data being processed.

7. How long do we keep your personal data?

We are keeping your personal data for a period of 30 days from the date of recording of the images. 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 legal/judicial and/or administrative proceedings. These are covered by other records.

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 access badges, will remain on the badge for as long as it is being used by the data subject (for the duration of the access badge validity) or until the data subject exercise his/her rights and objects it and withdraws his/her consent.

For identification data, the retention is set to be until termination of the link between the data subject and the Agency/EUIBA (the employer) plus 6 months and varies based on the type of link (e.g.

statutory staff: end of service / contract plus 6 months; external contractors: end of placement plus 6 months; visitor: end of visit plus 6 months; etc.).

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

8. WHAT ARE YOUR RIGHTS?

You have the right to access your personal data and may exercise your right of information / access / rectification / erasure / restriction / data portability / objection / withdrawal of consent by contacting the data controller at: REA-LSO@ec.europa.eu, EACEA-LSO@ec.europa.eu and at EISMEA-LSO@ec.europa.eu.

Your request to exercise one of the above rights will be dealt within **one month**. This period may be extended pursuant to Art 14.3 of the Regulation.

Your right to information, access, rectification, erasure, restriction or objection to processing, may be restricted only under certain specific conditions as set out in the applicable Restriction Decision for [REA](#), [for EACEA](#), [for EISMEA](#) in accordance with Article 25 of Regulation. Restrictions may also apply due to communication of a personal data breach or confidentiality of electronic communications.

9. CONTACT INFORMATION

In case you have any questions about the collection/processing of your personal data, you may contact the data controller who is responsible for this processing activity by using the following email address: REA-LSO@ec.europa.eu, EACEA-LSO@ec.europa.eu or EISMEA-LSO@ec.europa.eu.

You shall have the right of recourse at any time to the competent Data Protection Officer at REA Data Protection Officer (DPO): REA-DATA-PROTECTION-OFFICER@ec.europa.eu, EACEA: EACEA-data-protection@ec.europa.eu or EISMEA: EISMEA-DPO@ec.europa.eu and the European Data Protection Supervisor: EDPS@edps.europa.eu.