



RECORD OF PERSONAL DATA PROCESSING
“Access control to building Simon Bolivar 34 (SB34) and Video-Surveillance”

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 " Regulation")

Record n°

61

In accordance with Article 31 of the 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 the following processes:

- 1) Mandatory records under Art 31 of the Regulation*
- 2) Compliance check and risk screening*

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

- Regularization of a data processing activity already carried out.*
 - Record of a new data processing activity prior to its implementation.*
 - Change of a data processing activity.*
-

PART 1 (This part may be public) Name of the processing operation		
1	Creation and last update of this record (if applicable)	NA
2	Short description of the processing	Access control to building Simon Bolivar 34 (SB34) and Video-Surveillance- Analogue and Digital Storage
(This part may be public) Part 1 - Article 31 Record		
2a	Legal basis	<p>The processing operations on personal data are carried out under Article 5 (1) of the Regulation (EU) 2018/1725, lawfulness of processing:</p> <ul style="list-style-type: none"> (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); (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: <ul style="list-style-type: none"> - 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.
3	Function and contact details of the controller	<p>The controller is the European Research Executive Agency (REA), represented by its Director. For organisational reasons, the role of the data controller has been entrusted by the Director to the delegated controller and is exercised by REA Head of Department D 'Coordination and Support Services'</p> <p>The data controller may be contacted via functional mailbox: REA-LSO@ec.europa.eu</p>

4	Contact details of the Data Protection Officer (DPO)	REA-DATA-PROTECTION-OFFICER@ec.europa.eu
5	Name and contact details of joint controller (where applicable)	<p>Names and contact details of respective controllers/the Agencies:</p> <ol style="list-style-type: none"> 1. REA: Head of Department D ‘Coordination and Support Services’: REA-LSO@ec.europa.eu 2. EACEA: Head of Unit R.1 – “People, Workplace and Communication”: EACEA-LSO@ec.europa.eu 3. EISMEA: Head of Unit C.02 “Workplace, IT and Communication”: EISMEA-LSO@ec.europa.eu <p>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 on video-surveillance and ensure the legality of the filming and of the storage of the images. The service for video-surveillance is part of its security services in the SLA with the European Commission Directorate-General for Human Resources and Security (DG HR.DS)¹.</p>
6	Name and contact details of processor (where applicable)	<p>Processors are involved in the processing</p> <p><input checked="" type="checkbox"/> Yes <input type="checkbox"/> No</p> <p>European Commission, Directorate-General for Human Resources and Security (DG HR.DS): EC-SECURITY-ACCESS@ec.europa.eu EC-SECURITY-TECHNIQUE@ec.europa.eu</p> <p>The name of the subcontractor/s that HR.DS has/have hired is: ‘Protection Unit’ - Rue Campagne du Moulin 53/12 – 4470 Saint-Georges-sur-Meuse – Belgium² (sub-processor)</p>
7	Purpose of the processing	<p>The video-surveillance system is used for typical security and access control purposes, as part of the general management and functioning of the Agencies.</p> <p>For security purposes:</p> <p>To assist the Agencies in fulfilling its duty of care towards its staff members, contractors, visitors, and all other persons on its premises by processing images that allow monitoring the access to the building SB34, and certain related internal areas.</p> <p>The video-surveillance system is not used to track movements of employees or monitor other areas such as offices, canteens, kitchenettes, lounges, waiting rooms, toilets, showers or changing rooms.</p>

¹ [HR.DS](#)

² [Record of the European Commission \(DPR-EC-00654.2\)](#)

		<p>Access control to SB34:</p> <p>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 SB34 premises, identity controls on SB34 premises and preventing unauthorised persons from entering SB34 premises.</p> <p>For staff from the Agencies (badge and fingerprints or PIN code). 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.</p> <p>For staff from other EU institutions, bodies and other agencies (“EUIBAs”): they will have access by showing their badge.</p> <p>For visitors: Pre-registration, using a central web application (V-PASS). This processing is handled by DG HR.DS under the record DPR-EC-00655.3.</p> <p>For external contractors: a badge is provided by DG HR.DS to them.</p>
8	Description of the categories of data subjects	<p>Data subjects are any individual entering into the building:</p> <ul style="list-style-type: none"> • Internal to the organisation: All REA staff members passing through the filmed areas. • External to the organisation: All individuals passing through the filmed areas.
9	Description of personal data categories	<p>Categories of personal data:</p> <p>For the video-surveillance: images taken by the video-surveillance system concerning the physical characteristics of persons</p> <p>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.</p>
10	Retention time (time limit for keeping the personal data)	<p>REA applies the principles and retention periods indicated in Common Retention List of the Commission by analogy:</p> <p>For video-surveillance: 30 days from the date of recording of the images.</p>

		<p>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.</p> <p>The process of erasure after the retention period is automatic whereby media is overwritten on a “first-in, first-out” basis.</p> <p>For access control: Fingerprints, that have voluntarily been stored on badges (data subject’s consent is required), will remain on the access badges 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 exercises his/her rights to withdraw his/her consent.</p> <p>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.</p> <p>Is any further processing for archiving purposes in the public interest, historical, statistical, or scientific purposes envisaged? No</p>
11	Recipients of the data	<p>Access is always granted on a need-to-know basis.</p> <p>Who will have access to the data within the Agency and for which purposes?</p> <p>No one for images recorded by the live surveillance nor live images.</p> <p>Who will have access to the data outside the Agency and for which purpose?</p> <p>Access to live video-surveillance images and recordings is granted to security guards (under contract by DG HR.DS) on a “need-to-know” basis to react immediately to any dangerous situation or unlawful act. In some cases, they may view shots of a maximum two hours to be able to reach on the field any dangerous or infringing situation.</p> <p>The DG HR.DS staff responsible for managing video-surveillance and mandated Security Directorate investigators have access to live video-surveillance images and recordings of less than 24 hours and 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.</p> <p>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</p>

		<p>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.</p> <p>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.</p> <p>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)</p> <p>Outside the Agency, the recipients are:</p> <ul style="list-style-type: none"> • 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. <p>Personal data is stored on Commission servers located in the EU.</p> <p>The processing of personal data will not include automated decision-making (such as profiling).</p>
12	<p>Are there any transfers of personal data to third countries or international organisations? If so, to which ones and with which safeguards?</p>	<p>Personal data will not be transferred to third countries or international organisations.</p>
13	<p><u>General</u> description of the technical and organisational security measures</p>	<p>An access control and video-surveillance system are put in place to ensure a secure access control and protection of SB34 premises, information and assets, as well as protection of persons present inside SB34 premises. Security measures include appropriate access rights and access control. Access to real-time images and electronic recordings is restricted to authorised personnel from the contracting company and security personnel of the European Commission.</p>

		<p>PACS is a closed system and does not involve automated sharing with third parties. Where biometric data (only fingerprint data) are collected, these data are never stored on a database and do not transit over a network. Moreover, the current access badge displays significantly fewer personal data than the previous version, notably it does not show the personnel number, staff category or location of site/building.</p>
14	<u>Data subject rights/restrictions</u>	<p>A data subject can exercise his/her rights (Art 14-27 of the Regulation) by submitting a request concerning access, rectification, erasure, restriction, or objection to processing of their personal data to the Controller (Article 14 of Regulation) by sending their request to the Functional Mailbox: REA-LSO@ec.europa.eu.</p> <p>They may be restricted only under certain specific conditions as set out in the applicable <u>Restriction Decision</u> in accordance with Article 25 of the Regulation.</p> <p>Further to the above, data subjects may contact the REA Data Protection Officer (DPO): REA-DATA-PROTECTION-OFFICER@ec.europa.eu</p> <p>In case of conflict, complaints can be addressed to the European Data Protection Supervisor: EDPS@edps.europa.eu</p>
15	Information to data subjects/Data protection notice (DPN)	<p>A Data Protection Notice (DPN) relevant to this data processing activity is available on the intranet and the website of REA, EISMEA and EACEA.</p> <p>For REA DPN: <u>Privacy Statement SB34 Video-surveillance</u></p> <p>The DPN is also available in a paper format at the SB34 reception desk upon request.</p> <p>Individuals with access to the Commission's internal website may visit the DG HR.DS webpage dedicated to <u>video-surveillance</u> to have more information on their data processing.</p>

