



**RECORD OF PERSONAL DATA PROCESSING**  
**“Video-surveillance at Covent Garden (CCTV) – Digital and Analogical Storage”**

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°**

39

---

*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.*
-

<b>PART 1</b> (This part may be public) <b>Name of the processing operation</b>		
<b>1</b>	<b>Creation and last update of this record (if applicable)</b>	Created on 27/11/2012 (Ares (2012)1399392) – updated on 29/07/2020 (Ares(2020)3992917)
<b>2</b>	<b>Short description of the processing</b>	Video-surveillance Covent Garden – Analogue and Digital Storage – live images and recordings from security cameras undertaken by the DG HR Technical Security Unit
<b>(This part may be public)</b> <b>Part 1 - Article 31 Record</b>		
<b>2a</b>	<b>Legal basis</b>	<p>The processing operations on personal data are carried out under Article 5 (1) of the Regulation (EU) 2018/1725:</p> <p>(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; including processing of personal data necessary for the management and functioning of the Union Institutions or bodies (Recital (22) of the Regulation);</p> <p>(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:</p> <ul style="list-style-type: none"> <li>- Articles 8 and 21 of Commission Decision (EU, Euratom) 2015/443 of 13 March 2015 on Security in the Commission;</li> <li>- 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;</li> <li>- Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission.</li> <li>- Article 24 of the Staff Regulations of officials and the Conditions of Employment of other servants of the European Union.</li> </ul>
<b>3</b>	<b>Function and contact details of the controller</b>	<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: <a href="mailto:REA-LSO@ec.europa.eu">REA-LSO@ec.europa.eu</a></p>
<b>4</b>	<b>Contact details of the Data Protection Officer (DPO)</b>	<a href="mailto:REA-DATA-PROTECTION-OFFICER@ec.europa.eu">REA-DATA-PROTECTION-OFFICER@ec.europa.eu</a>

5	<b>Name and contact details of joint controller (where applicable)</b>	<p>Joint controllership is involved  <input checked="" type="checkbox"/>yes <input type="checkbox"/>no</p> <p>Names and contact details of respective joint controllers/the Agencies:</p> <ol style="list-style-type: none"> <li>1. European Research Executive Agency (REA): Head of Department D ‘Coordination and Support Services’: <a href="mailto:REA-LSO@ec.europa.eu">REA-LSO@ec.europa.eu</a></li> <li>2. European Research Executive Agency (ERCEA): Head of Unit D.2 – “Human Resources”: <a href="mailto:ERC-LSO@ec.europa.eu">ERC-LSO@ec.europa.eu</a></li> <li>3. European Health and Digital Executive Agency (HADEA): Head of Unit C.3 “Staff, Communication and Support”: <a href="mailto:HaDEA-LSO@ec.europa.eu">HaDEA-LSO@ec.europa.eu</a> (the Agencies”)</li> </ol> <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 video-surveillance and ensure the legality of the filming and 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)<sup>1</sup>.</p>
6	<b>Name and contact details of processor (where applicable)</b>	<p>Processors are involved in the processing  <input checked="" type="checkbox"/>yes <input type="checkbox"/>no</p> <p>European Commission, Directorate-General for Human Resources and Security (DG HR.DS):  <a href="mailto:EC-SECURITY-ACCESS@ec.europa.eu">EC-SECURITY-ACCESS@ec.europa.eu</a>  <a href="mailto:EC-SECURITY-TECHNIQUE@ec.europa.eu">EC-SECURITY-TECHNIQUE@ec.europa.eu</a></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 – Belgium 2  (sub-processor)</p>
7	<b>Purpose of the processing</b>	<p>The video-surveillance system is used for typical security purposes, as part of the general management and functioning of the Agencies. The video-surveillance system assists the Agencies in fulfilling its duty of care towards its staff members, contractors, visitors, and all other persons on its premises as well as the assets and the information of the Agencies by processing images that allow monitoring the access to the building complex, and certain internal areas of the buildings COV2 and COVE (REA uses COVE A premises floors 0-6 and 8-9).</p>

<sup>1</sup> [European Commission Video Surveillance Policy managed by HR.DS](#)

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

		<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> <p>This processing operation is also 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.</p>
8	<b>Description of the categories of data subjects</b>	<p>Data subjects are any individual entering into the building:</p> <ul style="list-style-type: none"> <li>• Internal to the organisation: All REA staff members passing through the filmed areas.</li> <li>• External to the organisation: All individuals passing through the filmed areas.</li> </ul>
9	<b>Description of personal data categories</b>	<p>Categories of personal data: images taken by the video-surveillance system 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.</p>
10	<b>Retention time (time limit for keeping the personal data)</b>	<p>REA applies the principles and retention periods indicated in <a href="#">Common Retention List of the Commission</a> by analogy:</p> <p>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>Is any further processing for archiving purposes in the public interest, historical, statistical, or scientific purposes envisaged?</p> <p><input type="checkbox"/>yes <input checked="" type="checkbox"/>no</p>
11	<b>Recipients of the data</b>	<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</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 HR Security Directorate 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 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’s 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.</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>
12	<b>Are there any transfers of personal data to third countries or international organisations? If so, to which ones and with which safeguards?</b>	<p>Data is transferred to countries outside the EU or EEA</p> <p>NA</p> <p>Data is transferred to international organisation(s)</p> <p>NA</p>
	<b><u>General</u> description of the technical and organisational security measures</b>	<p>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>
14	<b><u>Data subject rights/restrictions</u></b>	<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: <a href="mailto:REA-LSO@ec.europa.eu">REA-LSO@ec.europa.eu</a>.</p> <p>The request will be dealt within one month from receipt of the request. This period may be extended pursuant to Article 14(3) of Regulation (EU) 2018/1725.</p>

		<p>These rights 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): <u>REA-DATA-PROTECTION-OFFICER@ec.europa.eu</u></p> <p>In case of conflict, complaints can be addressed to the European Data Protection Supervisor: <u>EDPS@edps.europa.eu</u></p>
15	<p><b>Information to data subjects/Data protection notice (DPN)</b></p>	<p>A Data Protection Notice (DPN) relevant to this data processing activity is available on the intranet of REA, ERCEA and HaDEA.</p> <p>For REA DPN: <u>Privacy Statement COVE Video-surveillance</u></p> <p>For ERCEA DPN: <u>Video Surveillance System page</u></p> <p>For HaDEA DPN: <u>2023- 01 DPN videosurveillance.pdf</u></p> <p>The DPN is also available in a paper format at the COVE 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>

