

Record of data processing activities related to video-surveillance (CCTV) at European Institute of Innovation and Technology Premises

Nr	Item	Description
1	Reference number	DPO-05
2	Name of the data controller, the data protection officer and processor, if applicable and contact details	<p>The data controller is the Head of the Administration Unit.</p> <p>Contact e-mail: EIT-Buildingmanagement@eit.europa.eu.</p> <p>Contact e-mail of the Data Protection Officer: EIT-DPO@eit.europa.eu</p>
3	Purposes of the processing	<p>The purpose of the personal data processing is to ensure security and access control in the premises of the EIT by means of the video-surveillance. The electronic surveillance system allows direct observation, in which images and sound are being monitored and recorded.</p> <p>The system is not used for any other purpose, for example, it is not used to monitor the work of employees or to monitor attendance. Neither is the system used as an investigative tool (other than investigating physical security incidents such as thefts or unauthorised access). It is only in exceptional circumstances that the images may be transferred to investigatory bodies in the framework of a formal disciplinary or criminal investigation.</p>
4	Categories of data subjects	EIT staff (temporary agents, contractual agents, interims, SNEs, trainees), external visitors, maintenance, couriers and any other third parties entering the monitored area.

5	Categories of the personal data processed	<p>The video- surveillance system at the EIT premises captures images and sounds within monitored areas, which include commonly accessible spaces (e.g., near elevators, passages) that are clearly marked with specific pictograms containing both images and text.</p> <p>The location of the cameras was carefully reviewed to ensure that they minimise the monitoring of areas that are not relevant for the intended purposes. CCTV conducts monitoring on a limited scale (no facial recognition, coverage limited to entry/exit points, only on-premises, not in public space). Areas with heightened expectations of privacy, such as toilet facilities, leisure areas, individual and shared offices, and open-plan workspaces, are not subject to monitoring.</p> <p>The video surveillance system is not designed to capture, target, or process images revealing “special categories of personal data” as defined under Article 10 of Regulation 2018/1725.¹ (hereinafter “the Data Protection Regulation of the European Institutions”)</p> <p>While the primary purpose of the CCTV system is not to process such data, information related to ethnic or racial origin may be inadvertently captured. In such cases, the processing of this data is permitted under the exception outlined in paragraph 2(g) of Article 10 of the Data Protection Regulation of the European Institutions for reasons of substantial public interest, namely in the premises of EIT.</p>
6	Categories of data recipients	<ul style="list-style-type: none"> - Within the EIT: <ul style="list-style-type: none"> - The personal data of data subjects are processed by authorised EIT staff on a need-to-know basis, specifically by the Local Security Officer (LSO) and the Deputy LSO.

¹ OJ L 295, 21.11.2018, p. 39-98

		<ul style="list-style-type: none"> - The CCTV system operates autonomously, and no continuous monitoring or processing of data occurs. Access to and processing of recorded data is only carried out upon authorisation by the EIT Director or the Head of Administration. - Access to the personal data may be given to the Internal Control Coordinator of the EIT by request of the EIT Director if necessary and justified for the performance of the duties of the Internal Control. - Access to the personal data also may be given to the EIT Legal officers in context of administrative inquires and/or disciplinary proceedings. <p>- Within the Commission:</p> <ul style="list-style-type: none"> - The access to personal data may be granted to the Internal Audit Service of the Commission, Legal Service, OLAF upon request and only if necessary in the context of official investigations or for audit purposes. <p>Within other EU institutions and bodies:</p> <ul style="list-style-type: none"> - For the purpose of handling review procedures and litigation, access to the personal data may be granted to the European Ombudsman, the European Data Protection Supervisor, the General Court and the European Court of Justice upon request and to the extent necessary for handling the review procedure and litigation. <p>Third parties subject to the GDPR² and third parties not subject to the GDPR:</p> <ul style="list-style-type: none"> - Exceptionally, and only, if necessary (e.g., in the event of a security incident), personal data collected through video-surveillance at the EIT
--	--	---

² Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

		<p>premises may be disclosed to the relevant investigative or judicial authorities of the Member State in which the EIT premises are located.</p> <ul style="list-style-type: none"> - Exceptionally, and if necessary, personal data related to video-surveillance of the EIT premises (e.g. in case of investigations of criminal offences) may be disclosed to law firms. The respective data recipient will handle your personal data in accordance with the instructions of the Data Controller (EIT). The agreement between the parties will include relevant provisions regarding data protection.
7	Time limit storage	<p>Any video and sound footage captured by the camera system at the monitored area of the EIT premises will be stored and retained for a maximum of 30 days from the date of the recorded event. After this period, the data is deleted automatically. In case of an open investigation, a copy of the footage, if it was not deleted, will be made and stored until the investigation is closed.</p>
8	If applicable, transfers of personal data to a third country or to international organisation (if yes, the identification of that third country or international organization and the documentation of suitable safeguards)	No
10	General description of the technical and organisational security measures	<p>Organisational measures: restricting access to the personal data solely to authorised staff (LSO and Deputy LSO with prior authorisation of EIT Director or Head of Administration Unit) with a legitimate need-to-know for the purpose of this processing operation.</p> <p>Technical measures: All personal data in electronic format is stored on EIT servers, with restricted access to the server room. In addition, general security measures are</p>

		in place to ensure online security, prevent data loss, alteration, or unauthorized access.
11	For more information, including how to exercise rights to access, rectification, object and data portability (where applicable), see the data protection notice:	<p>Please consult the Data Protection page on the EIT's website:</p> <p>https://eit.europa.eu/who-we-are/legal-framework/data-protection</p>

Signature of the data controller

(Approval is given via a workflow in ARES in place of a handwritten signature)

Annex: Privacy statement