European Union Agency for Cybersecurity (ENISA)
Agamemnonos 14 | Chalandri 15231 | Attiki | Greece | info@enisa.europa.eu | www.enisa.europa.eu

TLP - CLEAR

Record No 20

Access Control to ENISA premises in Athens and Heraklion

Record 12 of processing operation "Access Control to ENISA premises in Athens and Heraklion"	
Date of last update	06/04/2026
Name and contact details of controller	ENISA, Corporate Support Services Unit (FCL), security [at] enisa.europa.eu
Name and contact details of DPO	dataprotection [at] enisa.europa.eu
Name and contact details of Joint Controller	N/A
Name and contact details of processor	• G4S Security company providing the security guard services, under a specific contract with ENISA; • ServiceNow Nederland B.V. Hoekenrode 3, 1102 BR, Amsterdam Zuidoost, (THE NETHERLANDS) under EC SIDE III FWC to which ENISA is also a party, as detailed under Record No. 90 – ServiceNow SFM.

Purpose of the processing	• Protection of ENISA's premises against unauthorized access and theft, as well as against external and internal threats, by:
	  ○ controlling general access to the building and specific access to different parts of the building (e.g. server room);
	  ○ using a badge with identification features, both for staff and visitors
	• Investigation of security-related incidents;
	• Generate list of persons, present in the building in the event of a building evacuation or any other emergency;
	• In justified cases, ensure accuracy of physical presence information. The reporting officer, may request a limited amount of access control data after notifying the staff member, to verify the accuracy of the data provided by staff on recording of working hours with the access data (dates and times of entering & leaving the premise) over a limited and notified period.

Description of data subjects	The data subjects are:

	• All ENISA staff (Temporary Agents / Contract Agents / SNE's / Trainees / Interim Agents). • Contractors, including intramuros • Visitors of ENISA premises.
Description of data categories	• Identification data of data subjects who have been issued a personalized badge: badge holder's first and last name, personnel number (if applicable), photo, function, badge expiry date, badge serial number, date, time and location where card is swiped. • Identification data of data subjects who receive a visitors badge: first and last name, ID card/passport number, date of visit, purpose of visit
Time limits (for the erasure of data)	• For personalized badge holders, identification data are retained for a period of 6 months after they leave ENISA. Data related to date, time and location where card is swiped are deleted after 6 months; • For visitor badges, identification data are retained for 185 days after the visit takes place and are then deleted; • For ensuring accurate information: the aforementioned retention periods apply, unless the data verification leads to a legal matter, the verification data may become subject to the retention time provided for the personal staff member file. The data received by the reporting officer shall then be deleted.
Data recipients	The Security Officer of the Agency and Facilities Management staff members (for visitors) and the security guards of G4S company in order to enable them to carry out their duties. In case of an incident, a list of events could be given to the Security Directorate of the EU Commission and/or local law-enforcement Authorities. In case of ensuring accurate information (only in justified cases and to support the verification over a limited period of the date and time of entering and leaving the building): the security officer providing the requested data, the reporting officer and the staff member, the HR staff for the purpose of filing and support in the case of a legal matter. The data may also be available to EU bodies charged with monitoring or inspection tasks in application of EU law (e.g. internal audits, European Anti-fraud Office – OLAF).
Transfers to third countries	No transfers outside EU/EEA are foreseen. Any transfer of personal data outside the EU/EEA is performed in compliance with Chapter V EUDPR.

Security measures - General description	General security policy and technical/organisational measures applicable to ENISA's internal IT systems and external platforms
Privacy statement	Available to ENISA intranet for all staff and to visitors during registration.