European Union Agency
for Cybersecurity

Agamemnonos 14
Chalandri 15231 | Attiki | Greece
Tel: +30 28 14 40 9711
E-mail: info@enisa.europa.eu
www.enisa.europa.eu

PROCEDURE ON PRESENCE MONITORING FOR EMERGENCY PURPOSES

Record of processing activity	
Title	Procedure on presence monitoring for emergency purposes
Name and contact details of controller	ENISA, Corporate Support Services (Facilities), security.officer@enisa.europa.eu
Name and contact details of DPO	dataprotection@enisa.europa.eu
Name and contact details of Joint Controller	N/A
Name and contact details of processor	G4S company, providing security services for ENISA (guards).
Purpose of the processing	Security of staff and visitors in ENISA building. In particular, to have a complete overview of people which are inside the building at a particular point in time for security purposes (so as for example to be able to evacuate the building during or after an emergency, such as a fire, earthquake etc.) In the context of the covid-19 pandemic, this process has been extended to apply for presence monitoring in case that a covid-19 case is reported by an ENISA staff member (who had been present in the office). In such case, all staff members that had been present in the office up to 14 days prior to the reported covid case, are accordingly informed by the ENISA security officer about the event (without disclosing the name of the staff member that tested positive) and given further guidance. This process is combined with an office occupancy and approval procedure via the ENISA's intranet: ENISA staff members are asked to declare two days before vising the office their presence in the ENISA's building; they can further visit the building after approval of the ENISA's security officer who monitors the number of allowed persons per building/area/office. Moreover, to enter the premises, it is mandatory to present one of the relevant covid-19 certificates to be checked by the security personnel (see record on Access control). Note: In addition, HR may disclose to the Security Officer and ENISA Security Guards the name of staff members reported sick with COVID-19, particularly for staff present in the office in the same period; the purpose of this disclosure is to enforce access control, as appropriate (see also related record for Reporting and handling of covid-19 cases). For staff becoming ill during teleworking no such information will be shared.
Description of data subjects	Employees. suppliers and visitors at ENISA's building in Athens.
Description of data categories	For the presence monitoring at ENISA's building: name and indicator of presence (in/out). No recording of time of arrival/departure. For the intranet-based office occupancy procedure: name of staff member, date of visit to the office, building/office space to be occupied.

Time limits (for the erasure of data)	Before the pandemic, retention was 24 hours (data destroyed at the end of each day by the ENISA guards). In the context of the pandemic, this period was extended to 14 days - in order to allow for proper information of ENISA staff in case of a reported covid-19 case.
Data recipients	a) The ENISA guards and the Security Officer have access to the data of presence monitoring at the buildings. b) ENISA HR receives a list of staff present per day by the guards, in order to follow-up the process in the event of a covid case. c) The office occupancy webpage is available to all staff members via ENISA's intranet.
Transfers to third countries	N/A
Security measures - General description	The paper-based presence sheet, which is maintained by security guards, is physically protected by the guards and is destroyed as per retention period by the ENISA guards. The office occupancy web page is protected by ENISA's intranet security measures.
Privacy statement	Information provided to all ENISA staff through intranet.