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

RECORD NO: 15

MANAGEMENT OF LEAVES FOR ENISA STAFF

Record 15 of processing operation "Management of leaves for ENISA staff"	
Date of last update	11/2/25
Name and contact details of controller	ENISA, Corporate Support Services Unit (HR), hr-general [at] enisa.europa.eu, Notif.Sickleave [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	• European Commission Sysper 2, DG HR, HR-MAIL-A3 [at] ec.europa.eu under a specific SLA between ENISA and the Commission for Sysper. • European Commission DG HR Medical Service (HR-BXL-CONGES-SPECIAUX-MED [at] ec.europa.eu and HR-BXL-CERTIFICATS-MEDICAUX [at] ec.europa.eu, under a specific SLA between ENISA and the Commission for conducting medical controls/checks to sick leaves, processing medical certificates and validate sick leaves and special leaves.
Purpose of the processing	ENISA uses the SYSPER 2 "Time Management" module which serves the management of leaves of Enisa's staff members (TA, CA and SNEs): Annual leave, special leave and sick leave and also leave rights and work patterns. With the purpose of validating sick and special leaves, do medical controls/checks to certified sick leaves, and process medical certificates. The processing operation includes communication of medical certificates by the staff member to the EC medical service. The Medical service sends in return to HR validation of sick leaves (without disclosing any medical data). For the medical controls/checks, the Medical service deals directly with the Staff member in question and only confirms to HR whether the sick leave is found to be justifiable or not. Upon receiving this information, HR encodes, when applicable, the relevant leave to SYSPER 2.
Description of data subjects	The data subjects are statutory (temporary agents, contract agents, seconded national experts) staff of ENISA.
Description of data categories	The following types of personal data are processed : • Annual leave: names, first names, staff number, date of absence, phone, address. • Special leave: names, first names, staff number, date of absence, phone, address, reason and supporting documents (if applicable). Supporting documents are requested for processing the validation of the above mentioned special leave cases. Examples of supporting documents: marriage certificate, birth certificates, medical certificates, death certificates, certificate of adoption, examination certificate, training certificate. In case of (very) serious illness of a partner/child/ascendant, if the needed supporting documentation reveals sensitive data it is possible

	to send the same info to the Medical Service of the European Commission.
	• Sick leave:
	  ○ For the absence without a certificate: name, surname, personal number, date of absence, address. The leave manager/gestionaire de conges (GECO) or the secretary of the unit introduces the sick leave in Sysper 2.
	  ○ For the absence with a medical certificate: the GECO receives a list only mentioning the name of the staff member, the length of the absence and the type of leave (sick leave, medical part time, etc).
	  ○ All other data mentioned on the medical certificates are exclusively processed by the medical service of the EU Commission.

Time limits (for the erasure of data)	• Data are generally kept for five years (more in cases of appeal) except where one of the time limits specified below is applicable. • Data relating to sick leave can be kept for at least three years pursuant to Article 59(4) of the Staff Regulations, but this time period is extended to five years in order to cover legal disputes. If a jobholder is transferred to another EU agency or institution suing SYSPER 2, only the data concerning sick leave in the previous five years are communicated. • The retention of data relating to days of annual leave is justified in particular for the carry-over of days not taken to the following year, but will be limited to two years (at the beginning of calendar year "n" the data for year "n-3" will be suppressed). • Data on part-time work, parental and family leave are generally kept at least until the end of active service in ENISA or even beyond that period (since they relate to a subsisting entitlement and may be appealed against). *Note #1: The data relating to the leaves of ENISA staff processed in other ENISA internal systems before the migration to SYSPER 2 shall follow the same retention periods.* *Note #2: If data are kept longer than the above-mentioned period, they will be rendered anonymous in SYSPER 2: the implementation of this action is at the moment under study by the Commission.*
Data recipients	ENISA authorised staff: line manager of the data subject (Head of Unit), Leave Managers(GECOs). European Commission SYSPER 2 and Medical Services authorized staff offering technical support related to the implementation and operation of SYSPER 2 modules, hosting of SYSPER 2 and other components, analysis of technical nature in relation to providing additional modules and services, assessment of medical certificates and special leaves supporting documents provided by staff members Authorised staff of the following EU institutions may have access to relevant personal data for audit control or investigation purposes: Court of Auditors, Internal Audit Service of the European Commission, European Anti-Fraud Office (OLAF). For the purpose of handling review procedures and litigation, access to the personal data may be granted also 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.
Transfers to third countries	No transfers outside EU/EEA are foreseen.
Security measures - General description	General security policy and technical/organisational measures applicable to ENISA's internal IT systems and technical security provisions laid down in the Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission, its subsequent versions, its implementing rules (as adapted from time to time) and the corresponding security standards and guidelines, as well as the Commission

	Decision (EU, Euratom) 2015/443 of 13 March 2015 on the security in the Commission, its implementing rules and the corresponding security notices.
Privacy statement	Available to all ENISA staff in intranet