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: 21

ADMINISTRATIVE INQUIRIES AND DISCIPLINARY PROCEDURES

Record 21 of processing operation "Administrative inquiries and disciplinary procedures"	
Date of last update	12/1/2026
Name and contact details of controller	ENISA, Corporate Support Services Unit (HR) & ENISA Appointing Authority, enisa-idp [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	N/A
Purpose of the processing	The purpose of this processing operation is the management of personal data dealt with during administrative inquiries and disciplinary procedures within ENISA, inline with ENISA MB DECISION No 2025/12. In particular, ENISA first processes the data in the context of the preliminary assessment (pre-inquiry). When the ENISA Appointing Authority is informed of a case with possible administrative or disciplinary dimension, it may further appoint an investigation panel, comprising of ENISA staff members and/or staff members of other EU institutions. The investigation panel, at the end of the assessment will issue a recommendation to the ENISA Appointing Authority (e.g. not to follow-up the case, refer the case to OLAF or organise a preliminary hearing). When an administrative inquiry is formally opened, the investigation panel has the powers to gather all necessary evidence and carry out inspections. *Note: In the context of the overall process, ENISA may be supported by EC IDOC (a specific Service Level Agreement is in place between ENISA and IDOC for this purpose) as regards advice on legal and procedural matters. If there is need to transfer information to IDOC, ENISA shall blackout all personal data and send only contextual information to IDOC, so as to receive the best possible legal and/or procedural advice.*
Description of data subjects	ENISA staff members (ENISA's servants and former servants within the meaning of the CEOS), National experts, persons employed under private law contracts and trainees; External (to ENISA) data subjects acting as investigator(s), inquiry (support) team member(s) during the process, witness(es), alleged victim(s), etc.
Description of data categories	For the preliminary assessment (pre-inquiry) stage: • Data qualified as "hard" or "objective" are factual, administrative information including identification data relating to those implicated in an inquiry or procedure; • Data qualified as "soft" or "subjective" are allegations and declarations by the affected individuals, which may also be based upon a reasonable suspicion or the subjective perception of the investigators;

	• Sensitive data (such as data concerning health, information revealing political opinions, etc.). For the administrative inquiry and disciplinary proceedings: • Confidentiality declarations signed by all officers involved in an administrative inquiry or disciplinary proceedings; • Disciplinary decision (provided by the ENISA investigation panel) stored in the personal file of the affected staff member; • Statements from staff members who may have information relevant to administrative inquiries either via a hearing or written statement; • The hearing that shall be recorded in a document signed by the staff member or any other person who was heard and by the interviewers once it has ended;Documents submitted by the staff member during the hearing; • Written conclusion following the completion of the administrative inquiry drawn by the investigation panel, which sets out the procedural steps followed by the facts and circumstances relevant to the case and, if appropriate, individual responsibilities; • The ENISA investigation panel draws recommendations on the appropriate follow-up measures. *Note: the personal data collected and processed is restricted to the necessary and proportionate for the purpose of establishing the facts and, where necessary, determining whether there has been a failure to comply with the obligations incumbent on ENISA staff members.*
Time limits (for the erasure of data)	• In the context of preliminary assessment and when the case is dismissed, the data is kept for a maximum of 2 years after the adoption of the decision that no inquiry will be launched; • In the context of the administrative inquiry file, including the collection of evidence and interviews of individuals, there are three possibilities: i) the inquiry is closed without follow-up, ii) a caution is issued or iii) the ENISA Appointing Authority adopts a formal decision that a disciplinary proceeding should be launched. For cases i) and ii), a maximum of five-year-period from closure of the investigation is considered to be a necessary retention period, taking into account audit purposes and legal recourses from the affected individuals. For case iii), ENISA shall transfer the inquiry file to the disciplinary file, as the disciplinary proceeding is launched on the basis of the evidence collected during the administrative inquiry. • In the context of pre-disciplinary proceedings, in line with Article 26 of the EC Decision C(2019) 4231 of 12.06.2019, where the ENISA Appointing Authority decides to address a warning to the person concerned pursuant to Article 3(1)(b) of Annex IX to the Staff Regulations, it shall be inserted in his or her personal file. The person concerned has the right to add comments on the warning, which shall also be inserted in the personal file. After 18 months of the date of the warning, the person concerned may ask the Appointing Authority to have it removed from his or her personal file. • In the context of disciplinary file, ENISA takes into consideration the nature of the sanction, possible legal recourses as well as audit purposes to set up a maximum retention period, after the adoption of the final Decision. If the decision acquits the staff member, it is retained in the personal file (10 years after the last pension) with the agreement of the staff member. If the decision imposes sanctions, the staff member may submit a request, under Article 27 of Annex IX to the Staff Regulations for the deletion, otherwise it is retained in the personal file (10 years after the last pension payment).
Data recipients	• ENISA Appointing Authority responsible for opening the administrative inquiry; ENISA heads of departments/units to the extent that this information is necessary for the performance of their tasks and on a strict “need-to-know” basis; ENISA HR representative or ENISA staff member(s) providing support during an administrative procedure; . • Investigation Panel or Disciplinary Board mandated by ENISA; • European Commission IDOC mandated to set out the purpose and scope of an administrative inquiry independently, to establish the facts and determine the

	individual responsibilities of the person concerned; This may apply within the context of the EC C(2019) 4231 and not within the framework of the SLA with ENISA (in such case IDOC acts as controller in itself). • EU or national bodies charged with monitoring or implementation of EU or national law (e.g. national courts, ECJ, etc.).
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.Disciplinary files and administrative investigation files are kept in a locked filling cabinet allowing to access solely to authorised individuals.The electronic files are saved on a secured drive, with limited access.
Privacy statement	Available on ENISA's intranet for all ENISA staff.