

RECORD NO: 69

MANAGEMENT AND PRESERVATION OF THE ENISA'S DOCUMENTS IN HERMES-ARES- NOMCOM (HAN)

Record 69 of processing operation “Management and preservation of the ENISA’s documents in Hermes-Ares-NomCom (HAN)”

Date of last update	22/05/2023
Name and contact details of controller	ENISA Executive Director’ Office, EDOoffice [at] enisa.europa.eu
Name and contact details of DPO	dataprotection [at] enisa.europa.eu
Name and contact details of Joint Controller	N/A. Note that EU-login (ECAS account), used for identification/authentication to the HAN, is provided by European Commission (DG DIGIT) directly (who acts as data controller to this end).
Name and contact details of processor	European Commission (Secretariat General and Directorate - General for Informatics - DG DIGIT.) The SG is the owner of the system, which is supplied by the DG DIGIT.
Purpose of the processing	The purpose of this processing activity is to provide the means to implement an effective policy for the electronic management and archiving of documents and files based on a Service Level Agreement signed between ENISA and the European Commission for the use of the Hermes-Ares-NomCom platform (HAN). This platform is for internal use only and is not accessible to third parties. In this way, ENISA plans to manage, store and find, reliably and at any time, any document relating to its official tasks, regardless of its medium (paper or electronic copy) or management system.
Description of data subjects	<ul style="list-style-type: none"> Internal - all ENISA members (including seconded national experts, interim staff, trainees, intra muros) External - Every individual who sends or receives documents that need to be captured or registered and every individual whose personal data are mentioned in said documents.
Description of data categories	<p>The following personal data are being processed:</p> <ul style="list-style-type: none"> Personal data in the metadata accompanying documents and files in HAN: <ul style="list-style-type: none"> a) Metadata in relation to the author and addressee of a given document: <ul style="list-style-type: none"> - For a HAN user (at ENISA it concerns all temporary and contract staff, seconded national experts, interim staff, trainees, intra muros): first name and surname, the administrative entity to which the user is linked, unit, COMREF



	<p>person ID, the work email address and any other kind of personal data added to the free text comments fields and titles.</p> <p>- For an external natural person that is sender or addressee of a given document the personal data that can be encoded are: First name (optional), surname (mandatory), email address (mandatory), city in which that person is located (optional), country in which that person is located (optional), organisation for which that person is working (optional), webpage (optional), and any other kind of personal data added to the free text comments fields</p> <p>b) The title or subject of the document or file concerned may contain any category of personal data and typically reflects the title or subject indicated by the author of the document or the service responsible for managing the file;</p> <p>c) The title/brief description of the attachments of the document concerned may contain any category of personal data.</p> <ul style="list-style-type: none"> • Personal data in the audit trail and workflow data in HAN (relating to HAN users only since external natural persons have no access to HAN): <ul style="list-style-type: none"> a) Workflow actions: First name and surname (mandatory), the administrative entity to which the person is linked (mandatory). b) Audit trail: EU Login user login and administrative entity to which the user is linked • Personal data in access management and control data in HAN (relating to HAN users only since external natural persons have no access to HAN): User ID, first name, surname, the administrative entity to which the person is linked and e-mail address as imported from COMREF with an indication of the type of individual access rights of a user. • Personal data in document content in HAN (to ensure authoritative records, for full text search and for the (organisation of the) transfer of files to the historical archives): The documents processed may contain any category of personal data that was provided by the person writing the document.
<p>Time limits (for the erasure of data)</p>	<p>Personal data will be kept the time necessary to fulfil the purpose of collection or further processing, namely:</p> <ul style="list-style-type: none"> • Personal data in mandatory metadata in relation to any document: namely metadata about the author and addressee of a given document (typically name and surname of the respective individuals and the department/body to which they belong), metadata about the title or subject of a given document, metadata about the attachments (brief description) and metadata in relation to the title of the file in which it is filed are kept indefinitely to ensure that: <ul style="list-style-type: none"> (a) ENISA can meet its legal obligations, including those relating to public access to documents and the maintenance of historical archives, (b) the validity of the electronic or digitised documents can be guaranteed for as long as the documents are stored, and (c) once these documents have been eliminated, ENISA is still able to retrieve the documents' metadata to be able to explain that the documents have been eliminated and have evidence on the procedure followed. • Personal data in audit trail and workflow data are kept indefinitely to ensure that the authors and participants in major records management actions at the level of metadata, documents, files or procedures can be identified even after elimination of the documents concerned. • Personal data in access management and control data are kept for as long as the user works for ENISA. • Personal data in document content are kept throughout the specific retention period that has been defined for the document (based on the specific data processing activity that the document relates to). Retention periods for all types of documents in HAN are specified in a dedicated retention list for ENISA.
<p>Data recipients</p>	<p>Access to your data will be granted only to all temporary and contract staff, seconded national experts, interim staff, trainees, intra muros, at ENISA responsible for carrying out this processing operation. 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).</p>

Transfers to third countries	No transfers outside EU/EEA is foreseen.
Security measures - General description	In accordance with Article 33 of Regulation (EU) 2018/1725, the Commission as, data processor, has adopted and implemented technical, security and organisational measures for the electronic records management system Hermes-Ares-NomCom (HAN) to ensure the security of the personal data processed. Such measures cover system inherent features, and functionalities made available, and apply to data in transit and stored. They include also data logging.
Privacy statement	It will be provided to users within the ARES system.

