European Institute for Gender Equality

Data protection notice on the management and (short- and medium-term) preservation of the EIGE's documents in Hermes-Ares-NomCom (HAN)

Last updated: 20 March 2025

The European Institute for Gender Equality (EIGE) is committed to protect your personal data and to respect your privacy. EIGE collects and further processes personal data pursuant to Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data (repealing Regulation (EC) No 45/2001).

You will find information in this document pertaining to the processing of your personal data by EIGE. If, upon reading it, you still have questions, please contact us at:

EIGE's Data Protection Officer, dpo@eige.europa.eu
EIGE's Document Management Officer, ares@eige.europa.eu

Purpose of processing

EIGE collects and uses your personal data to respond to several essential needs of the Agency:

- ensure business continuity in and accountability on the Agencies' activities by keeping appropriate documentation about them, and contribute to the transparency of its activities to European citizens;
- improve internal service quality with document management, collaboration and workflow features; and
- preserve the institutional memory of the Agency, through long-term preservation of certain types of files for archiving purposes.

Managing and (temporarily) preserving (storing) documents (including personal data) in Hermes[1]-Ares[2]-NomCom[3] is usually not why the personal data were collected and processed in the first place. The temporary storage of documents (and the personal data they contain) in Hermes-Ares-NomCom is a processing activity that forms an integral part of the original

[1] Hermes is the common electronic file repository used by all the directorates-general and services of the Commission for the Commission's current and intermediate records.
[2] Ares is the web application, connected to Hermes, that is used to register and file documents in the Commission.
[3] NomCom is the web application, connected to Hermes, that is used to manage the Commission's filing plan, file lists, retention lists and the appraisal and transfer of files to the Commission's historical archives.

processing operation under which the personal data were collected and processed in the first place. Such temporary storage follows a specific retention period in line with the Retention List[4] and the processing falls outside this processing operation.

The processing under the present processing operation covers the processing activities that go beyond the storage of the content of documents and is necessary for the following specific reasons:

- Ensure that documents are authoritative records of the Agency by accompanying them by contextual data (so called 'metadata', including personal data such as names) that explicitly document their critical characteristics;
- Ensure that documents are traceable (including by means of personal data such as names). EIGE needs to be able to clearly and definitely identify the documents it has written or received. It needs to be able to trace them throughout their lifecycle and manage them in the context in which they were written or received. For these related aspects, the processing of mandatory minimum metadata about the author and the addressee of a given document is necessary (Article 3 of EIGE's Document Management Policy[5]);
- Ensure that appropriate techniques and security measures are adopted to ensure IT security of the systems used for records management, including the maintenance and update of these systems;
- Enable access management and access control based on the predefined rights of users and owner departments of documents and on the level of accessibility to the documents themselves. To achieve this, the name of any EIGE staff member may be processed and the EIGE staff member who is granted access rights to the document concerned may access any personal data the document contains; and
- Enable processing for archiving purposes in the public interest by organising and ensuring the transfer of files to the Commission's Historical Archives Service in line with the retention policies set out in the Agency's Specific Retention List.

Your personal data will not be used for any automated decision-making including profiling.

Legal basis of processing

EIGE processes your personal data since it is necessary for the management and functioning of the Agency[6], as well as to comply with legal obligation which are imposed upon EIGE[7], namely by:

- Treaty on the Functioning of the European Union, namely Articles 15 and 298;
- Charter of Fundamental Rights of the European Union, namely Article 41;
- Council Regulation (EEC, Euratom) No 354/83 concerning the opening to the public of the historical archives of the European Economic Community and the European Atomic Energy Community, and more in particular Articles 1(2)(a) and 7;

[4] The Retention List presents the retentions schedule for each category of files

[5] Adopted by Director's Decision No 325 of 29 October 2024.

[6] Processing is, therefore, justified for the performance of a task carried out in the public interests, as allowed by Article5(1)(a) of Regulation (EU) 2018/1725.

[7] Article 5(1)(b) of Regulation (EU) 2018/1725.

- Regulation (EC) 1049/2001 of the European Parliament and of the Council regarding public access to European Parliament, Council and Commission documents, and more in particular Articles Article 2(3) and 11(1);
- Management Board Decision No MB/2013/006 of 14 June 2013 on Policy on Public Access to Documents at the European institute for Gender Equality; and
- Director's Decision No 325 of 29 October 2024 on EIGE's Document Management Policy.

Types of personal data collected

The title/description of documents and their content may contain any category of personal data. They may appear in files relative to human resources management, financial management, health management, management of disciplinary proceedings (e.g., identification data, financial data, HR data, medical data and social data).

EIGE may process the following special categories of personal data as listed under Article 10 of the Regulation:

- Data revealing racial or ethnic origin;
- Data revealing political opinions;
- Data revealing religious or philosophical beliefs;
- Data revealing trade union membership;
- Data concerning health; and
- Data concerning a natural person's sex life or sexual orientation.

Depending on the circumstances of the case, processing of personal data will be done as:

- necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security[8];
- [9];
- it relates to personal data which are manifestly made public by the data subject[10];
- necessary for the establishment, exercise or defence of legal claims or whenever the Court of Justice of the European Union is acting in its judicial capacity[11];
- necessary for reasons of substantial public interest, on the basis of Union law which shall be proportionate to the aim pursued[12];
- necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union law or pursuant to contract with a health professional[13]; and

[8] Article 10(2)(b) of Regulation (EU) 2018/1725.
[9] Article 10(2)(c) of Regulation (EU) 2018/1725.
[10] Article 10(2)(e) of Regulation (EU) 2018/1725.
[11] Article 10(2)(f) of Regulation (EU) 2018/1725.
[12] Article 10(2)(g) of Regulation (EU) 2018/1725.
[13] Article 10(2)(h) of Regulation (EU) 2018/1725.

- necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes[14].

In order to carry out this processing operation, EIGE collects the following categories of personal data:

a). Personal data in the metadata accompanying documents and files in HAN:

- Metadata in relation to the author and addressee of a given document:
  For a HAN user[15] that is stakeholder of a document the personal data that are present are: first name and surname, the administrative entity to which the user is linked, the internal phone number extension, the office location, the COMREF person ID[16], the work email address (if enabled) and any other kind of personal data added to the free text comments fields.
  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 (optional or mandatory[17]), city in which that person is located (optional), country in which that person is located (optional), organisation for which that person is working (optional) and any other kind of personal data added to the free text comments fields.
- 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.
- The title/brief description of the attachments of the document concerned may contain any category of personal data.

b. 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):

- Workflow actions: First name and surname (mandatory), the administrative entity to which the person is linked (mandatory). The internal phone number extension and office location are displayed when encoding or consulting but not stored in the system.
- Audit trail: EU Login[18] user login and administrative entity to which the user is linked.

[14] Article 10(2)(j) of Regulation (EU) 2018/1725.

[15] Each staff member in the Agency can be a HAN user, irrespective of whether (s)he actively uses the system or not.

[16] COMREF stands for Common Reference and is a database in which all staff reference data are gathered for EU institutions, agencies and bodies. The database is used as an official provider of human resources data for information systems. COMREF is connected to HAN and fed by Sysper2, which is the IT system used by EU institutions, agencies and bodies to manage aspects of human resources. The COMREF person ID is only visible to those HAN users assigned a Document Management Officer (DMO) profile in HAN.

[17] A person's email address becomes mandatory information when an incoming or outgoing email is encoded using the AresLook plugin in O.utlook and when Ares documents are sent to an external natural person directly via Ares using the external transmission functionality.

[18] EU Login is the system used by the Commission, EU bodies and agencies to authenticate users of internal IT systems. This system offers centralised authentication of users with various levels of guarantee concerning the person providing authentication details.

c. 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.

Individuals who have access to the data

Access to personal data is provided to EIGE staff responsible for carrying out this processing operation and to authorised staff according to the "need to know" principle. Such staff abide by statutory, and when required, additional confidentiality agreements.

Concerning the possible processing of special categories of personal data and other sensitive personal data, access is managed via a triple security: at level of metadata there is minimal encoding, at the level of a given document security markings are applied to restrict visibility and at the level of the files the access to a given file's content is restricted to people or services that have a need to know.

Access to personal data in document content is given to those persons or organisations outside EIGE that are recipients of documents that have been sent in the context of its activities. Personal data will be shared only when they are necessary in the context of the activity and in accordance with the rules and conditions of Regulation (EU) 2018/1725.

The Agency may send a document to a recipient residing in any country outside the EU/EEA territory. Apart from the recipient's own personal data, EIGE only discloses personal data to a recipient residing outside the EU if the conditions for an international transfer of Chapter V of Regulation (EU) 2018/1725 are met. It is the responsibility of the controller responsible for the specific processing to ensure that the conditions of Chapter V of Regulation (EU) 2018/1725 are met.

Pursuant to point (13) of Article 3 of Regulation (EU) 2018/1725, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients. The further processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.

No other third parties will have access to your personal data, except if required by law.

Retention policy

EIGE only keeps your personal data for the time necessary to fulfil the purpose of collection or further processing, namely:

- 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 a) that the Agency can meet its legal obligations regarding public

access to documents and concerning the opening to the public of its historical archives, b) that the validity of the electronic or digitised documents can be guaranteed for as long as they are stored, and c) that once these documents have been eliminated the Agency 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 EIGE; and
- Personal data in document content are kept throughout the retention period, as defined in the common retention list, of the file in which the de-facto controller has filed the document.

Security of your personal data

All personal data in electronic format (e-mails, documents, databases, uploaded batches of data, etc.) are stored either on the servers of the Agency or of its contractors. All processing operations are carried out pursuant to Commission decision (EU, EURATOM) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission.

The Agency's contractors are bound by a specific contractual clause for any processing operations of your data on behalf of the Agency, and by the confidentiality obligations deriving from the Regulation (EU) 2018/1725.

In order to protect your personal data, EIGE has put in place a number of technical and organisational measures covering the use of Ares-NomCom. Technical measures include appropriate actions to address online security, risk of data loss, alteration of data or unauthorised access, taking into consideration the risk presented by the processing and the nature of the personal data being processed. Organisational measures include restricting access to the personal data solely to authorised persons with a legitimate need to know for the purposes of this processing operation.

The definition of who does what in which type of document and which type of file is vital in all records management systems. This access is managed in HAN via the combination of access right principles with the use of roles and profiles.

a) Based on the 'need to know principle' end users of HAN only have the right to access certain documents and files on which they only do a limited number of actions.
The access rights in HAN are based on the following principles:
When a document is saved in HAN (meaning the document is still under preparation) the document is only accessible to its creator.

- When a saved document is put in a workflow (e-signatory or assignment) by its creator, the document is only available to its creator and the workflow actors;
- As soon as a document is registered, it becomes visible (accessible in read mode) to all stakeholders concerned (creator + workflow actors + sender(s) + recipient(s)); and
- As soon as a document (saved or registered) is filed in a file, access to this document (in read mode) is also given to all persons that have File Reader right on that file. In which file a document is filed defines the increased visibility of the document. The widest visibility in HAN is Agency visibility. A document filed in a file with Agency visibility is visible to all EIGE HAN users unless the creator has indicated that it contains sensitive personal data or a marking is applied. Each document has to be filed in at least one file. A saved document that is not filed is destroyed after six months.

b) Based on which role(s) they have been assigned end users of HAN can access certain documents and files and perform actions on these.
   The roles in HAN are managed as follows:
   - A limited number of specific users 'administrators' give end users access rights to documents and files and rights to perform actions. This type of security management is called Role-Based Access Control (RBAC)[19];
   - The roles are assigned to the headings of the filing plan, to the files and to the documents in HAN;
   - A role and the access rights it entails includes all subordinate roles and rights. For example, for the headings, a heading editor automatically has the rights of heading editor, file creator and heading reader;
   - Main roles for the headings of the filing plan are: none (= the end user does not know the heading exists), heading reader (= the end user knows the heading exists and what its metadata are but cannot create files under the heading), file creator (= the end user can create files under the heading but cannot modify the heading. The end user will be file editor for the files created) and heading editor (= the end user can modify a heading, its metadata, its access rights and can created subheadings);
   - Main roles for the files are: none (= the end user does not know the file exists), file reader (= the end user knows the file exists and see its content but cannot file documents in the file), filing user (= the end user can file documents in the file but cannot modify the file) and file editor (= the end user can modify the metadata of the file, its access rights and can create subfiles).

[19] Since HAN has many users and the number of operations that can be performed is long, access rights management is simplified by creating groups of users and group the operations they can perform in 'roles'. Groups are created for functional reasons (e.g. DMO) or organisational reasons (e.g. ADM) and a user can belong to several groups and have several roles. The users and organisational groups are managed in the system via an automatic import from SYSPER2 and COMREF. For functional groups and roles, there is no automatic procedure in place so managing these manually is necessary.

- Main roles for the documents are: none (= the end user does not know the document exists), read (= the end user can see the content of a document but cannot update it), version (= the end user can modify the metadata and content of the document but only by creating a new version of the document) and write (= the end user can modify the metadata and the content of the current version of a document);
- The role file reader on a file automatically gives read right on all documents filed in this file unless a document has a marking to limit access to it. A marking on a document in HAN gives access restriction directly on the document because it determines the persons and/or groups that have exclusive access to the document. Documents with marking are accessible to their stakeholders but upon their filing, they only become available to users that are file reader and belong to the group of users20 that can read that particular marking. In practice, this means that as soon as a document is filed in a file with Commission visibility, access to this document (in read mode) is given to all HAN users in the Commission unless a specific marking is attached to it that limits access to it;
- End users can only register documents when they have the generic register role; and
- The Agency's DMO is the 'Role Manager' that manages the roles centrally (which roles can perform which actions).

c) Right to perform operations on the basis of profiles:
Users are grouped in profiles and to each profile a number of operations (system roles) is linked. This way end users or groups of end users that have permissions to perform similar operations are grouped under one single name. The profiles define what operations users can perform on the documents to which they have the access that their security role establishes.

The profiles in HAN are as follows:

- A no Ares access user cannot connect to Ares, not even in read mode;
- A base user can save, file and search, create external entities[21] and create distribution lists and workflow lists for personal use;
- A normal user can save, file, search and register, create external entities and create distribution lists and workflow lists for personal use;
- An advanced user can save, file, search and register, create external entities, create distribution lists and workflow lists for unit/directorate use and manage deadlines;

[20] For each marking, HAN has a marking group indicating which users can apply this marking to a document or access a document with the marking in question. DMO profiles can consult and manage (i.e. add and/or delete) members from the security markings SENSITIVE and SPECIAL HANDLING ("to read" and "to apply") and from the working groups. Users with a DMO profile can manage members for the markings and for the working groups.

[21] The external entities functionality in Ares gathers all data relating to non-HAN users and organisations encoded into the system by HAN users, and allows for the management of these data.

- An advanced secretary user can save, file, search and register, create external entities, create distribution lists and workflow lists for unit use, manage deadlines and own virtual entities;
- A CAD user can save, file, search and register, create and manage external entities, create distribution lists at all levels and workflow lists for unit and Agency use, manage deadlines, manage the Agency's virtual entities, do a modify special on a registered document and annul the validity of a registered document;
- A DMO user can save, file, search and register, create and manage external entities, create distribution lists at all levels and workflow lists for unit and Agency use, manage deadlines, manage the Agency's virtual entities, do a modify special on a registered document and annul the validity of a registered document, as well as actions related to the use of Ares (profile assignment, managing marking groups, reports,…); and
- Users can delegate their profile in Ares (user delegation). They can fully or partially delegate all they can see in Ares (documents, tasks, received documents, etc.) as well as all they can do (their delegates can then create documents on their behalf). They can define several delegates, either individuals or virtual entities. For each delegate they define for how long the delegation is valid and what the delegate can do. Users can also delegate certain types of tasks, based on their action code (used in the document assignment and the document validation workflow), either to a person or to a virtual entity (task delegation). As a consequence, the specified tasks are automatically sent to the user they have delegated these tasks to.

Your rights as data subject

Within the limits set by Regulation (EU) 2018/1725, you have the right to access, rectify, erase and/or port your personal data, as well as to restrict or object to the processing of your personal data.

In order to exercise your rights, please contact ares@eige.europa.eu whereby you shall specify your claim (i.e. the right(s) you wish to exercise). The exercise of your rights is free of charge. If your request is manifestly unfounded or excessive, EIGE may refuse to act on it.

Insofar the right to object to the processing of your personal data is concerned, the exercise of that right has to be based on grounds relating to your particular situation.

You can exercise your rights by contacting the Data Controller, or in case of conflict the Agency's Data Protection Officer.

Other rights

Should you feel that the processing infringes the data protection rules, you are entitled to raise a complaint with the European Data Protection Supervisor.