



Privacy Statement for document management and (short- and medium-term) preservation in Hermes-Ares-NomCom (HAN)

The purpose of this document is to describe how CEPOL complies with its obligations to protect personal data under Regulation (EU) 2018/1725¹ and to provide individuals with information about CEPOL's processing of personal data and their rights under the Regulation.

This privacy statement concerns the processing operation "Management and (short- and medium-term) preservation of CEPOL's documents in Hermes - Ares - NomCom (HAN)", undertaken by the Document Management Officers, as corporate controllers, as well as by all other organisational entities of CEPOL that conduct part of the processing under this processing operation ('de-facto controllers').

What is the purpose of the processing?

CEPOL process personal data while managing and temporarily preserving documents to respond to a number of essential needs of the institution:

- Ensure continuity and accountability on CEPOL's activities by keeping appropriate documentation about them and contribute to the transparency of CEPOL's activities to the citizen.
- Improve internal service quality with document management, collaboration and workflow features.
- Preserve the institutional memory of CEPOL, through long-term preservation of certain types of files for archiving purposes.

The processing of data for the management and preservation of CEPOL documents using HAN (HERMES-ARES-NOMCOM) system is necessary for the following reasons:

1. Ensure that documents are authoritative records of CEPOL by accompanying them contextual data ('metadata',) documenting their critical characteristics.
2. Ensure that documents are traceable throughout their lifecycle and CEPOL clearly and definitely can identify the documents 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.
3. Ensure compliance with the Agency's Document Management Policy.
4. 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.
5. Enable access management and access control based on the predefined rights of users and owner departments of documents. To achieve this, the name of any CEPOL

¹ 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, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, OJ L 295, 21.11.2018, p. 39–98.

Privacy Statement	Document number: FO.DAPR.001-1
	Approval date: 21.03.2024

staff member may be processed and the CEPOL staff member who is granted access rights may access any personal data the document contains.

6. Enable processing for archiving purposes in the public interest in line with the retention policies.

What is the legal basis for the processing of personal data?

Processing personal data in the context of document management is necessary for compliance with a legal obligation of EU law to which the Agency is subject. In particular,

- **Regulation (EU) 2018/1725** and in particular Article 5.
- **Commission decision (EU) 2021/2121** on records management and archives
- **Common Commission-level retention list** for European Commission files: SEC(2007)970, SEC(2012)713, SEC(2019)900 and SEC(2022)400.
- **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
- **Regulation (EC) 1049/2001** of the European Parliament and of the Council regarding public access to European Parliament, Council and Commission documents

Although the HAN system does not process special categories of data for the managing and preservation of CEPOL documents, it might be that the content of the documents managed includes special categories of data pursuant to under Article 10(1)² of Regulation (EU) 2018/1725. In that case, the legal basis for the processing of special categories of data will depend on the category of personal data and the purpose for which the data were collected and processed in the first place and would fall under any of the exceptions of Article 10(2) of Regulation (EU) 2018/1725.

Who is the data controller?

The data controller is the Head of Corporate Services Unit, (HeadofCSU@cepol.europa.eu) of CEPOL.

Who are the data subjects?

All end users of HAN, accordingly CEPOL staff members (as creators and workflow actors) and any person who sends to or receives from CEPOL a formal document which is registered in the system.

Which types of data are being processed?

The title/description of documents and their content may contain any category of personal data³. More specifically, the following categories of personal data is collected:

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 that is stakeholder of a document these include first name and surname, the unit to which the user is linked, the internal phone number extension, the office location, the COMREF person ID, the work email address.

² Data revealing racial or ethnic origin, political opinions religious or philosophical beliefs, trade union membership, data concerning health, a natural person's sex life or sexual orientation.

³ They may appear in files related to human resource management, financial management, health management, management of disciplinary proceedings (identification data, financial data, HR data, medical data, social data).

Privacy Statement	Document number: FO.DAPR.001-1
	Approval date: 21.03.2024

- For an external natural person that is sender or addressee of a given document the personal data that can be first name, surname, email address, and optionally the city, country in which that person is located, organisation for which that person is working.
- 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.

Personal data in the audit trail and workflow data in HAN

- For workflow actions on a mandatory basis these are first name and surname, the unit to which the person is linked. E-mail address of the author(s) or participant(s) involved in major records management actions at the level of metadata, documents, files or procedures (e.g. document signing, document transmission, responsibility for a given file or for transfer of a given file to the historical archives).
- For audit trail these personal data are EU Login user login and the unit to which the user is linked.

Personal data in access management and control data in HAN

- User ID, first name, surname, the unit 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.

How is data processed?

The temporary storage of documents (and the personal data they contain) in Hermes-Ares-NomCom is a processing activity that is an integral part of the original processing operation under which the personal data were collected and processed. Such temporary storage follows a specific retention period in line with the CEPOL's Specific Retention List and the processing falls outside this processing operation.

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. When a document is saved in HAN 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 to all stakeholders concerned (creator + workflow actors + sender(s) + recipient(s)). As soon as a document 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 CEPOL visibility. A document filed in a file with CEPOL visibility is visible to all CEPOL HAN users unless the creator has indicated that it contains sensitive personal data, or a marking is applied.

Privacy Statement	Document number: FO.DAPR.001-1
	Approval date: 21.03.2024

Based on which role(s) they have been assigned end users of HAN can access certain documents and files and perform actions on these. A limited number of specific users 'administrators' give end users access rights to documents and files and rights to perform actions. The roles are assigned to the headings of the filing plan, to the files and to the documents in HAN.

- Main roles for the headings of the filing plan are: none, heading reader, file creator, and heading editor.
- Main roles for the files are: none, file reader, filing user, and file editor.
- Main roles for the documents are: none, read, version and write.
- 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 which determines the persons and/or groups that have exclusive access to the document.
- End users can only register documents when they have the generic register role.
- CEPOL has one or several 'Role Managers' that manage the roles centrally (which roles can perform which actions) and assign the 'Profile Manager' role to specific users in each Unit, who then assign roles to functional and organisational groups.

Regarding the right to perform operations based on profiles, users are grouped in profiles and to each profile several operations (system roles) is linked. 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 can be *no Ares access* (cannot connect to Ares), *base user* and *normal user* (can save, file, search, create external entities⁴ and create distribution/workflow lists), *advanced user* (can save, file, search and register, create external entities, create distribution/workflow lists for unit/directorate use and manage deadlines), *advanced secretary user* (same rights as an advanced user complemented with managing own virtual entities), *CAD user* (same rights as the advanced secretary user complemented with managing the Agency's virtual entities, modifying a registered document and annul the validity of a registered document), *DMO* (has the rights of all the above users complemented with doing actions related to the use of Ares (profile assignment, managing marking groups, reports,...)).

Users can delegate their profile in Ares and 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.

Who are the recipients of the data being processed?

Access to personal data is provided to CEPOL staff responsible for carrying out the processing operation and to authorised staff according to the "need to know" principle. Such staff abide by statutory, and when required, additional confidentiality agreements. Full access is only assigned to the administrator of the application. Staff who are involved in a workflow or a case have access to the related files.

Outside CEPOL, data can be accessed by all persons that are recipients of documents that have been sent by the Agency in the context of its activities. The actual organisational entity responsible for the activity, as de facto controller, will share personal data only when they are

⁴ 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.

Privacy Statement

Document number: FO.DAPR.001-1

Approval date: 21.03.2024



necessary in the context of the activity and in accordance with the rules and conditions of Regulation (EU) 2018/1725. 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.

Is data transferred to third countries or international organisations?

Apart from the recipient's own personal data, CEPOL only discloses personal data to a recipient residing outside the EU if the conditions for an international transfer of Chapter V Article 47 and 48 of Regulation (EU) 2018/1725 are met.

What rights do data subjects have?

Data subjects have rights enlisted in Chapter III (Articles 14-25) of Regulation (EU) 2018/1725. In particular the right to access their personal data and to rectify them in case the personal data are inaccurate or incomplete. Under certain conditions, data subjects have the right to erase their personal data, to restrict the processing of their personal data, to object to the processing and the right to data portability, and they also have the right to receive their personal data in a structured, commonly used and machine-readable format.

Substantiated requests should be emailed to HeadofCSU@cepol.europa.eu. The time limit to block/erase data on justified grounds at the request of data subjects is 15 working days from the date of receipt of such a request.

General requests can be emailed to the CEPOL Data Protection Officer at DPO@cepol.europa.eu

How long is your data retained by CEPOL?

CEPOL 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 is kept indefinitely. In particular: metadata about the author and addressee of a given document, 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.
- 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 CEPOL.
- 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.

Privacy Statement	Document number: FO.DAPR.001-1
	Approval date: 21.03.2024

[Who should you contact for more information on the processing of your personal data by the Agency?](#)

Data Protection Officer (DPO)

Within CEPOL, there is a data protection officer. This person is independently responsible for ensuring the internal application of Regulation (EU) 2018/1725 and that the rights and freedoms of the data subjects are not likely to be adversely affected by the processing operations. The DPO keeps a register of all processing operations of personal data carried out by the Agency.

The DPO also provides advice and makes recommendations on rights and obligations of data controllers and data subjects. CEPOL's DPO can be contacted at DPO@cepol.europa.eu.

European Data Protection Supervisor (EDPS)

The [European Data Protection Supervisor](#) is an independent supervisory authority with responsibility for monitoring and ensuring the application of data protection rules by EU Institutions and Bodies, which includes CEPOL. The EDPS provides advice to EU Institutions and Bodies on all matters relating to the processing of personal information and cooperates with national supervisory authorities to improve protection of personal information.

[What should you do if you believe your data is being misused by the Agency?](#)

If you believe your data is being misused by CEPOL or is otherwise not compliant with your rights and freedoms under Regulation (EU) 2018/1725, you should notify the data controller (HeadofCSU@cepol.europa.eu). You may also inform the Agency's DPO to inform him/her of any issues related to the processing of your data. If the problem is not rectified after contact with the data controller and DPO, every data subject has the right of recourse to lodge a complaint with the EDPS, as provided for by Article 63 of Regulation (EU) 2018/1725.