Privacy Policy related to records and archives management

This privacy policy governs the processing of your personal data on the basis of the European Regulation (EU) N°2018/1725 ("**EUI-GDPR**") by **Key Digital Technologies Joint Undertaking ("KDT JU"),** set up by Council Regulation (EU) 2021/2085 of 19 November 2021, in the context of records and archives management. More specifically, it concerns the processing operation 'Records and archive management of KDT JU's documents' in the context of the use of HAN tools from the Commission.

What is the purpose of the processing?

On the basis of the EUI-GDPR, KDT JU collects and uses your personal data to respond to a number of essential needs:

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

Why and how do we collect your personal data?

The processing covers the processing activities that go beyond the storage of the content of records and is necessary for the following specific reasons:

- Ensure that documents are official records of the JU by accompanying them by contextual data (so called 'metadata', including personal data such as names) that explicitly document their critical characteristics.
- Ensure that records are traceable (including by means of personal data such as names). The JU needs to be able to clearly and definitely identify the records it has created or received. It needs to be able to trace them throughout their lifecycle and manage them in the context in which they were created or received.

- Enable access management and access control based on the predefined rights of users and owner of records and on the level of accessibility to the records themselves. To achieve this, the name of any staff member may be processed and the staff member who is granted access rights to the record concerned may access any personal data the records contains.

- Enable processing for archiving purposes in the public interest by organising and ensuring the transfer of files to the Historical Archives Service in line with the retention list.

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

Legal basis

The processing operation is justified on the following grounds:

- **KDT Records and Archives Management Policy**, setting rules on the management of records and archives in KDT JU.

- **Annex 7 of KDT GB 2021.02** approving Implementing Rules to Regulation (EC) No 1049/2001 regarding **public access to documents**: all EU citizens have the right to request documents from the EU institutions.

- **Annex 11 of KDT GB 2021.02** adopting the revised **Internal Control Standards** and putting the obligation to have appropriate information and document management systems in place. In particular, principle 13 specifies some of the features that these systems need to have.

- **Annex 12 of KDT GB 2021.02** updating the Financial Rules of the JU defining specific requirements for the retention of records supporting financial operations.

- **Data Protection Regulation 2018/1725 for EU institutions**. The Regulation puts more emphasis on the correct handling of personal data in IT systems. It defines a number of principles for designing or selecting IT systems, the relation with individuals whose data is processed or stored and the necessary measures in case a data breach occurs. All information management systems that process personal data have to comply with these principles. For the electronic document and records management systems the following points are especially relevant: privacy by data base design, clear information about the processing available to the data subject, consent of data subjects, and procedures in place in case of breaches.

- **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 the following articles:

    - Article 1(2)(a): 'Community archives' means all those documents and records of whatever type and in whatever medium which have originated in or been received by one of the institutions or by their representatives or servants in the performance of their duties, which relate to the activities of the European Economic Community and/or the European Atomic Energy Community (hereinafter referred to as 'the European Communities').

    - Article 7: 'Each institution shall transfer to the historical archives all documents and records contained in their current archives no later than 15 years after their date of creation. According to the criteria laid down by each institution pursuant to Article 9, there shall be an initial sorting process with the purpose of separating documents and records that are to be preserved from those that have no administrative or historical value.'

- **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 the following articles:

    - Article 2(3): 'This Regulation shall apply to all documents held by an institution, that is to say, documents drawn up or received by it and in its possession, in all areas of activity of the European Union.'

    - Article 11(1): 'To make citizens' rights under this Regulation effective, each institution shall provide public access to a register of documents. Access to the register should be provided in electronic form. References to documents shall be recorded in the register without delay.'

Which personal data we collect and further process?

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

Personal data in the metadata accompanying records and files in HAN:

- Mandatory minimum metadata in relation to the author and addressee of a given record: typically name and surname of the respective individuals and the unit to which they belong;

    - For a HAN user that is stakeholder of a record the personal data that are present are: first name and surname, 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 record the personal data that can be encoded are: First name (optional), surname (mandatory), email address (optional or 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) and any other kind of personal data added to the free text comments fields.

- The title or subject of the record or file concerned may contain any category of personal data and typically reflects the title or subject indicated by the author of the record or the service responsible for managing the file;

- The title/brief description of the attachments of the record concerned may contain any category of personal data.

<u>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):</u>

- Workflow actions: Name, surname, unit, e-mail address of the author(s) or participant(s) involved in major records management actions at the level of metadata, records, files or procedures (e.g. record signing, record transmission, responsibility for a given file or for transfer of a given file to the historical archives).

- Audit trail: EU login user.

<u>Personal data in access management and control data in HAN (relating to HAN users only since external natural persons have no access to HAN):</u>

- User ID, first name, surname, unit, e-mail address and individual access rights of a user may be processed.

<u>Personal data in record's content in HAN (to ensure authoritative records, for full text search and for the transfer of files to the historical archives):</u>

- The records processed may contain any category of personal data that was provided by the person creating the record.

How long do we keep your personal data?

The JU 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 record**: namely metadata about the author and addressee of a given record (typically name and surname of the respective individuals and the unit to which they belong), metadata about the title or subject of a given record, 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 JU 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 records can be guaranteed for as long as they are stored, and c) that once these records have been eliminated the JU is still able to retrieve the records' metadata to be able to explain that the records 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, records, files or procedures can be identified even after elimination of the records concerned.

- **Personal data in access management and control data** are kept for as long as the user works for the JU.

- **Personal data in record's content** are kept throughout the retention period, as defined in the JU retention list, of the file in which the de-facto controller has filed the record.

How do we protect and safeguard your personal data?

All personal data in electronic format (e-mails, records, databases, uploaded batches of data, etc.) are stored either on the servers of the JU or of the Commission in charge of managing HAN.

The JU's contractors are bound by a specific contractual clause for any processing operations of your data on behalf of the JU, and by the confidentiality obligations deriving from the General Data Protection Regulation in the EU Member States ('GDPR' Regulation (EU) 2016/679).

In order to protect your personal data, the Commission has put in place a number of technical and organisational measures covering the use of Ares-NomCom, including 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 record is put in a workflow (e-signatory or assignment) by its creator, the record is only available to its creator and the workflow actors.

   - As soon as a record is registered, it becomes visible (accessible in read mode) to all stakeholders concerned (creator + workflow actors + sender(s) + recipient(s)).

   - As soon as a record (saved or registered) is filed in a file, access to this record (in read mode) is also given to all persons that have File Reader right on that file[1]. In which file a record is filed defines the increased visibility of the record. The widest visibility in HAN is JU visibility. A record filed in a file with JU visibility is visible to all JU HAN users unless the creator has indicated that it contains sensitive personal data or a marking is applied. Each record has to be filed in at least one file. A saved record 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 records and files and perform actions on these.

[1] Depending on the content and sensitivity of the file, this right may be assigned to a single person, several persons, a unit or the whole JU.

The roles in HAN are managed as follows:

- A limited number of specific users ‘administrators’ give end users access rights to records and files and rights to perform actions. This type of security management is called Role-Based Access Control (RBAC).

- The roles are assigned to the headings of the filing plan, to the files and to the records 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 records in the file), filing user (= the end user can file records 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).

- Main roles for the records are: none (= the end user does not know the record exists), read (= the end user can see the content of a record but cannot update it), version (= the end user can modify the metadata and content of the record but only by creating a new version of the record) and write (= the end user can modify the metadata and the content of the current version of a record).

- The role file reader on a file automatically gives read right on all records filed in this file unless a record has a marking to limit access to it. A marking on a record in HAN gives access restriction directly on the record because it determines the persons and/or groups that have exclusive access to the record. Records 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 users that can read that

particular marking. In practice, this means that as soon as a record is filed in a file with JU visibility, access to this record (in read mode) is given to all HAN users in the JU unless a specific marking is attached to it that limits access to it.

- End users can only register records when they have the generic register role.

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 records 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 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 use and manage deadlines.
- An ***advanced secretary user*** can save, file, search and register, create external entities, create distributions 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 use, manage deadlines, manage the JU 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 use, manage deadlines, manage the JU'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 making groups, reports…).

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.

Who has access to your personal data and to whom is it disclosed?

Access to your personal data is provided to the 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, access is managed via a triple security: at level of metadata there is minimal encoding, at the level of a given record 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 that have a need to know.

Access to your personal data in the record's content is given to those persons or organisations outside the JU that are recipients of records that have been sent in the context of its activities. The actual service responsible for the activity will share your personal data only when they are necessary in the context of the activity.

The information we collect will not be given to any third party, except to the extent and for the purpose we may be required to do so by law.

What are your rights and how can you exercise them?

You have specific rights as a 'data subject' under Chapter III (Articles 14-25) of Regulation (EU) 2018/1725, in particular:

- the right to access your personal data and to rectify them in case your personal data are inaccurate or incomplete.

- Under certain conditions, you have the right to erase your personal data, to restrict the processing of your personal data, to object to the processing and the right to data portability.

- 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.

In light of article 25(1) of Regulation (EU) 2018/1725, as implemented in Annex 6 of KDT GB 2021.02, the JU may restrict some of the above rights in duly justified cases. These justified cases entail processing operations in the performance of:

- administrative inquiries;
- disciplinary proceedings;
- preliminary activities related to cases of potential irregularities deported to OLAF;
- whistleblowing procedures;
- procedures of harassment;
- processing internal and external complaints;
- internal audits;
- investigations carried out by the Data Protection Officer; or
- security investigations.

If you wish to request any information about data protection of exercise any of your rights as a data subject, you can contact us via e-mail at dpo@kdt-ju.europa.eu. An e-mail requesting to exercise a right will not be construed as consent with the processing of your personal data beyond what is required for handling your request. Such request should meet the following conditions:

- State clearly which right you wish to exercise; and
- your request should be accompanied by a digitally scanned copy of your valid identity card proving your identity.

We will promptly inform you of having received your request. If the request meets the conditions above and proves valid, we will honour it as soon as reasonably possible and at the latest thirty (30) days after having received your request.

If you have any complaints regarding the processing of your personal data by us, you may always contact us by sending an e-mail to dpo@kdt-ju.europa.eu. If you remain unsatisfied with our response, you are free to file a complaint with the European Data Protection Supervisor (https://edps.europa.eu).

More information on Data Protection at the JU can be obtained in the Record of Processing Activities and in the privacy notices published on the JU's website.