EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

RECORD OF PROCESSING ACTIVITY ACCORDING TO ARTICLE 31 REGULATION 2018/1725[1] NOTIFICATION TO THE DATA PROTECTION OFFICER

NAME OF PROCESSING OPERATION[2]: Management and (short- and medium-term) preservation of FRA documents by HAN (HERMES-ARES-NOMCOM) system

Reference number: DPR-2023-184
Creation date of this record: 22/05/2023
Last update of this record: 22/05/2023
Version:1

Part 1 (Publicly available)

1) Controller(s)[3] of data processing operation (Article 31.1(a))
Controller: European Union Agency for Fundamental Rights (FRA)
Schwarzenbergplatz 11, A-1040 Vienna, Austria
Telephone: +43 1 580 30 – 0
Email: contact@fra.europa.eu
Organisational unit **responsible**[4] for the processing activity: Corporate Services Unit
Contact details: *han@fra.europa.eu*
Data Protection Officer (DPO): dpo@fra.europa.eu

2) Who is actually conducting the processing? (Article 31.1(a))[5]	
The data is processed by the FRA itself	☒
The data is processed also by a third party (contractor)	☒

1 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1725

2 **Personal data** is any information relating to an identified or identifiable natural person, i.e. someone who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity. This information may, for example, be the name, date of birth, a telephone number, biometric data, medical data, a picture, professional details, etc.
Processing means any operation or set of operations which is performed on personal data, whether or not by automatic means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

3 In case of more than one controller (e.g. joint FRA research), all controllers need to be listed here

4 This is the unit that decides that the processing takes place and why.

5 Is the FRA itself conducting the processing? Or has a provider been contracted?

European Commission Secretariat-General (SG.C.1 - Transparency, Document Management & Access to Documents (SG-DATA-PROTECTION-COORDINATOR@ec.europa.eu) on the basis of an SLA signed between FRA and the European Commission.

3) Purpose of the processing (Article 31.1(b))

Why are the personal data being processed? Please provide a very concise description of what you intend to achieve with the processing operation. Specify the rationale and underlying reason for the processing and describe the individual steps used for the processing. If you do this on a specific legal basis, mention it as well (e.g. staff regulations for selection procedures).

The purpose of the processing operation in the context of document management via Hermes-Ares-NomCom (HAN) (document management tool managed by the European Commission) in the Agency is mainly the following:

- Ensure continuity and accountability in the context of the Agency activities by keeping appropriate documentation on them and contribute to the transparency of Agency activities to the citizen.
- Improve quality of services with document management, collaboration and workflow features.
- Preserve the institutional memory of the Agency, through long term preservation of certain categories of files for archiving purposes.

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

1. Ensure that documents are authoritative records of the Agency (meaning that they have reliability, integrity, usability and authenticity) accompanying them by metadata (including by means of personal data such as names) that explicitly document their critical characteristics.
2. Ensure the traceability of documents (including by means of personal data such as names) to be able to clearly and definitely identify the documents created or received so they can be traced throughout their lifecycle and managed in the context in which they were created or received.
3. Ensure compliance with the Agency's Document Management (PO.QMS.001) policy and Document and Records process (PR.QMS.005).
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 and on the level of accessibility to the documents themselves.
6. Enable processing for archiving purposes in the public interest in line with the retention policies

EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

4) Description of the categories of data subjects (Article 31.1(c))

Whose personal data are being processed?

FRA staff ☒

Non-FRA staff ☒

(Every individual who sends or receives documents that need to be captured or registered in line with Agency's Document management policy and the Document and Records process and every individual whose personal data are mentioned in said documents)

5) Categories of personal data processed (Article 31.1(c))

Please tick all that apply and give details where appropriate

We will collect only the following personal data necessary for the processing operation described above.

Personal data in the metadata accompanying documents and files:

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

- Name, surname, department, 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).

Personal data in access management and control data:

- Name, surname, department, e-mail address and individual access rights of a user may be processed.

Personal data in document content (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, for example:

(a) **General personal data**

Personal details

Contact details ☒

Education & Training details ☒

Employment details ☒

Financial details ☒

Family, lifestyle and social circumstances ☒

(b) **Special categories of personal data** (Article 10)
The personal data collected reveal:

Racial or ethnic origin ☒

Political opinions ☒

Religious or philosophical beliefs ☒

Trade union membership ☒

Genetic, biometric or data concerning health ☒

Information regarding an individual's sex life or sexual orientation ☒

N/A ☐

(c) **Personal data relating to criminal convictions and offences** (Article 11)

Criminal record (or similar, e.g. declaration of good conduct) ☐

N/A ☐

NOTE: The above special categories of data could be included in the documents registered in HAN.

6) Recipient(s) of the data (Article 31.1 (d))

*Recipients are all parties who have access to the personal data. Who will have access to the data **within** FRA? Who will have access to the data **outside** FRA? No need to mention entities that may have access in the course of a particular investigation (e.g. OLAF, EO, EDPS).*

Designated **FRA** staff members ☒

- All FRA staff that are involved in the processing to achieve the specific purposes of this processing operation (set out in Section 3) are granted access on a 'need to know' basis depending on the tasks to be carried out.
- Full access is assigned to the administrator of the application. Staff who are involved in a workflow have access to the related files. All staff can access and use the system. Access to data is restricted to those staff members involved in a particular file /electronic workflow.

Recipients **outside** FRA: ☒

- All persons outside the Agency that are recipients of documents that have been sent by the Agency in the context of its activities. External recipients are EUIBAs who are using HAN.
- Developers and helpdesk in Secretariat-General (SG) of the European Commission who need access to the data to solve bugs, to test new developments or for user research and usability tests.
- Data can also be transferred for specific purposes of control to the auditing or inquiring bodies like the Internal Audit of the European Commission, OLAF or the Court of Auditors, EDPS, etc. in respect of the provisions of the Regulation (EU) 2018/1725.

7) Transfers to third countries or international organisations (Article 31.1 (e))[6]

If the personal data are transferred outside the European Economic Area or to international organisations, this needs to be specifically mentioned, since it increases the risks of the processing operation.

Transfer outside of the EU or EEA

Yes ☐

No ☒

If yes, specify to which country:

Transfer to international organisation(s)

Yes ☐

No ☒

If yes specify to which organisation:

Legal base for the data transfer

☐ Transfer on the basis of the European Commission's adequacy decision (Article 47)

☐ Transfer subject to appropriate safeguards (Article 48.2 and .3), specify:

a) ☐ A legally binding and enforceable instrument between public authorities or bodies.

Standard data protection clauses, adopted by

b) ☐ the Commission, or

[6] **Processor** in a third country using standard contractual clauses, a third-country public authority you cooperate with based on a treaty. If needed, consult your DPO for more information on how to ensure safeguards.

c) ☐ the European Data Protection Supervisor and approved by the Commission, pursuant to the examination procedure referred to in Article 96(2) .

d) ☐Binding corporate rules, ☐ Codes of conduct , ☐ Certification mechanism pursuant to points (b), (e) and (f) of Article 46(2) of Regulation (EU) 2016/679, where the processor is not a Union institution or body.

Subject to the authorisation from the European Data Protection Supervisor:
☐ Contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation.

☐ Administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.

☐ Transfer based on an international agreement (Article 49), specify:

Derogations for specific situations (Article 50.1 (a) –(g))

☐ N /A
☐ Yes, derogation(s) for specific situations in accordance with article 50.1 (a) –(g) apply
In the absence of an adequacy decision, or of appropriate safeguards, transfer of personal data to a third country or an international organisation is based on the following condition(s):

☐ (a) The data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards
☐ (b) The transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request
☐ (c) The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person
☐ (d) The transfer is necessary for important reasons of public interest
☐ (e) The transfer is necessary for the establishment, exercise or defence of legal claims
☐ (f) The transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent
☐ (g) The transfer is made from a register which, according to Union law, is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down in Union law for consultation are fulfilled in the particular case

8) Retention time (Article 4(e))

How long will the data be retained and what is the justification for the retention period? Please indicate the starting point and differentiate between categories of persons or data where needed (e.g., in selection procedures candidates who made it onto the reserve list vs. those who didn`t). Are the data limited according to the adage "as long as necessary, as short as possible"?

- **Personal data in mandatory metadata in relation to any document (**metadata about the author and addressee of a given document, typically name and surname 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: Indefinitely in order to:
  - meet the Agency legal obligations regarding public access to documents and concerning the opening to the public of its historical archives
  - guarantee the validity of the electronic or digitised documents for as long as they are stored.
  - be able to retrieve the documents' metadata once these documents have been eliminated to explain that the documents have been eliminated and have evidence on the procedure followed

- **Personal data in audit trail and workflow data:** Indefinitely (as 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:** For as long as the user works for the Agency (as they are necessary for the proper functioning of document management, namely, to grant access to specific documents and exercise access control on documents)

  Personal data in document content: Throughout the retention period, as defined in the common retention list, of the file in which the de facto controller has filed the document

For more detailed information on the retention periods above, please refer to the data protection notice of the processor here.

9) Technical and organisational security measures (Article 31.1(g))

Please specify where/how the data are stored during and after the processing; please describe the security measures taken by FRA or by the contractor

How is the data stored?

Document Management System (DMS)	☐
FRA network shared drive	☐
Outlook Folder(s)	☐
CRM	☐
Hardcopy file	☐
Cloud (give details, e.g. cloud provider)	☐
Servers of external provider	☒

Data is stored in the Commission's Data Centre and are therefore protected by a number of measures introduced by the Commission to protect the integrity and confidentiality of the data.

Other (please specify):

10) Exercising the rights of the data subject (Article 14 (2))

How can people contact you if they want to know what you have about them, want to correct or delete the data, have it blocked or oppose to the processing? How will you react?

See further details in the Data Protection notice: e-mail to han@fra.europa.eu

Data subject rights

- ☒ Right of access
- ☒ Right to rectification
- ☒ Right to erasure (right to be forgotten)
- ☒ Right to restriction of processing
- ☐ Right to data portability
- ☒ Right to object
- ☒ Notification obligation regarding rectification or erasure of personal data or restriction of processing
- ☒ Right to have recourse
- ☐ Right to withdraw consent at any time