

**RECORD OF PROCESSING ACTIVITY
ACCORDING TO ARTICLE 31 REGULATION 2018/1725¹
NOTIFICATION TO THE DATA PROTECTION OFFICER**

NAME OF PROCESSING OPERATION²: Requests for internal and external training activities via the FRA training application

Reference number: DPR-2023-188 (to be completed by the DPO)
Creation date of this record: 23/06/2023
Last update of this record: 23/06/2023
Version: 1

Part 1 (Publicly available)

1) Controller(s)³ of data processing operation (Article 31.1(a))
<p>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 responsible⁴ for the processing activity: Corporate Services Unit Contact details: career@fra.europa.eu Data Protection Officer (DPO): dpo@fra.europa.eu</p>

2) Who is actually conducting the processing? (Article 31.1(a))⁵
<p>The data is processed by FRA itself <input checked="" type="checkbox"/></p> <p>The data is processed also by a third party (contractor) <input type="checkbox"/></p>

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?

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 processing the data is to optimise the processing of training requests from staff and to make the procedure easier for both staff requesting training and staff responsible for handling the requests. All staff training requests, for both in-house and external training activities, will be submitted via a central platform built in SharePoint, which allows management to approve applications and HR to monitor budget, consumption of learning days and learning needs.

The principle behind it is the continuous development of the skill set, knowledge, and learning capacity of staff, to improve their performance and, consequently, the Agency's, as well as to keep pace with change.

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

Whose personal data are being processed?

FRA staff (including TA, CA, SNE, trainees)

Non-FRA staff (personal data of natural persons providing the training could be processed when the staff member submits the training request when the training provider is registered in the trainer's name)

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

Please tick all that apply and give details where appropriate

(a) General personal data

Personal details (name and surname)

Contact details (FRA email address)

Education & Training details: Data related to the training activity itself

Employment details (unit (within FRA) and line manager)

Financial details (e.g. financial identification form, bank account information)

Family, lifestyle and social circumstances

Goods or services provided

Other (please give details):

- Professional skills and competences to be developed
- Personal data of natural persons providing the training could be processed when the staff member submits the training request if the training provider is registered in the trainer's name.
- A check box indicates whether the learning need was identified in the competency scan and/or CDP.

(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

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

- The staff member's superior, i.e. the Director or their Head of Unit, for the approval or rejection of the training activity request;
- The staff in CS in charge of training, on a need to know basis in order to check the availability of budget and learning days per staff member and give approval;
- The Head of Corporate Services Unit, for the final approval or rejection of the training activity request.
- IT staff members in charge of maintenance of the app

Recipients **outside** FRA:

(please provide a generic/functional mailbox)

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

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

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.

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 defense 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"?

In line with the Commission's Common Retention List, the data on learning and development activities is retained for 10 years after the year of the training activity.

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	<input type="checkbox"/>
Cloud (MS 365 SharePoint - record)	<input checked="" type="checkbox"/>
Servers of external provider	<input type="checkbox"/>
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?

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