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]: *FRA e-learning platform*

Reference number: DPR-2025-242 (to be completed by the DPO)
Creation date of this record: 08/08/2025
Last update of this record:
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: Communications and Awareness Raising Unit Contact details: *webfeedback@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) [mention the third party]	☒

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?

Processors:

- FRA's hosting contractor (MainStrat in consortium with Sarenet S.A.U.) as the data is stored on secure servers in the EU by the contractor.
- FRA's webservices contractor (Eworx) which acts as processor for software development tasks.

Contact point at external third party (e.g. Privacy/Data Protection Officer – use functional mailboxes, not personal ones, as far as possible):

- MainStrat: Security-DPO-Notifications@mainstrat.com
- Sarenet: protecciondedatos@sarenet.es
- Eworx, project mailbox email: dpo@eworx.gr

Separate controller:

- YouTube for videos which are viewed on the platform

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).

FRA's eLearning platform is a digital tool used to deliver and manage online learning content. It contains educational content, such as courses, videos, quizzes, and other interactive materials, to users. The platform aims to provide a flexible and engaging way for individuals to learn, whether for professional development, academic pursuits, or personal enrichment.

The purpose of the processing of personal data is to provide the e-learning platform with necessary information to help users manage their learning experience. This information is collected for the purposes of providing training and showing your progress through the activities offered in the e-learning platform (e.g. courses, quizzes and activities taken).

FRA's e-learning platform uses Moodle software to provide the Virtual Learning Environment (VLE). Moodle software is installed on web servers which are managed by FRA's hosting contractor at their data centres in Spain. The VLE software itself is maintained and customised by FRA's webservices contractor.

FRA records and uses your personal information via the Moodle software to:

- Provide you an account on, and identify you within, the VLE system
- Provide you access to courses/sites within Moodle
- Provide you the ability to upload, amend and delete certain information within Moodle
- Provide you access to the information, resources and activities uploaded to Moodle
- Control access to different parts of the system
- Help support Moodle users
- For system administration and bug tracking

- Report on course, resource and activity access, activity completion, course completion and course data (such as grades, scores, submissions and content uploaded)
- For producing usage statistics for management and planning purposes

When users register with the e-learning platform, they are asked to provide the personal data mentioned in section 5 below, which will serve to identify them as a user in the system. This includes information necessary to create the user profile. Other information, non-mandatory to use the e-leaning platform, can be provided by the user in their profile settings. This information can be modified or deleted at any time by the user.

Personal data for the user profile mentioned in section 5 below is collected during the registration process. The data collected is on the user learning experience, how far the user advances in each course, the quizzes and activities they take and their performance in such course elements.

When the user uses the e-learning platform, cookies are used to remember their username between pages and to store any settings they may have saved. The session cookie is called MoodleSession and is stored until they close the session by logging out or closing the browser. If they access a page with a YouTube video embedded on it, YouTube will also set cookies on their computer or mobile device. The platform also collects the Last IP address. This address is used to identify spam or malicious user creation.

Moodle logs contain detailed information about user activity within each course, including the date and time of when course-specific information was viewed and/or updated, the address of the machine from which the access was made, the browser identification information and information about the referring web page. Logs are used to create summary statistics which may be made publicly available. Summary statistics do not include personal data.

Information about contributions to courses, including contributions to chat rooms and discussion forums, ownership of resources, assignment/file submissions, text matching scores and evidence of participation in other Moodle-based activities is held within the Moodle system.

Information and data related to users, including grades, feedback comments, scores, completion data, access rights and group membership is also recorded.

The user may request a copy of all of their personal data. Once the request is processed, they will receive a notification to inform them that their personal data may be downloaded from their Data requests page. The user has by default one week to download their data before the download link expires.

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

Whose personal data are being processed?

FRA staff	☒
Non-FRA staff (please specify e.g. Roma community, judges, etc.)	☒

Users who register to participate in an e-learning course on Moodle, which is installed on a FRA server at the premises of the hosting contractor in Spain.

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

Please tick all that apply and give details where appropriate

(a) **General personal data (add or delete as appropriate – the data in the brackets are only examples)**

Personal details (Mandatory: username, password, first name, surname) ☒

Contact details
(Mandatory: email address; ☒
Optional: City/town, country, description, user picture, additional names, ID, Phone, Mobile phone, Address, Skype ID, Web page. Optional information is not part of the registration form but can be added by the user in their profile.)

Education & Training details ☐

Employment details ☒
(Optional: Institution, Department. Optional information is not part of the registration form but can be added by the user in their profile.)

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

Family, lifestyle and social circumstances (Optional: Interests. Optional information is not part of the registration form but can be added by the user in their profile.) ☒

Goods or services provided ☐

Other (please give details): ☒

Username – Mandatory field, can be a pseudonym

IP address – the last IP address of the user: The IP address is hidden from normal users. It is visible only to Moodle admins and available in the logs.

Actions taken by the user when on the e-Learning platform for example when a user completes a quiz or accesses a module. This information is used to generate statistics about course usage.

When you register with the e-learning platform, you will be asked to provide personal data, which will serve to identify you as a user in the system. This includes information necessary to create your user profile: a valid email address, a personal username which will be your user ID, and your first name and surname. Other information, non-mandatory to use the e-learning platform, can be provided by you in your “profile settings”. This information can be modified or deleted at any time by you. The fields in profile settings are the default set of fields in Moodle which come with the standard download package. They have not been customized by FRA.

Cookies:
MoodleSession (Mandatory) – A Moodle session cookie which is set by the e-learning platform and is deleted after the session expires. This cookie ensures that a users' session is maintained when navigating through the website. If the user does not use the session cookie they would have to re-login on every page.

YouTube (Mandatory) The other 4 cookies are the following YouTube cookies if the user accesses a page which has embedded YouTube videos:
GPS - Registers a unique ID on mobile devices to enable tracking based on geographical GPS location. – Duration 1 day
PREF - Registers a unique ID that is used by Google to keep statistics of how the visitor uses YouTube videos across different websites. – Duration 8 months
VISITOR_INFO1_LIVE - Tries to estimate the users' bandwidth on pages with integrated YouTube videos – Duration 179 days
YSC - Registers a unique ID to keep statistics of what videos from YouTube the user has seen. – Deleted after end of session.

(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 (please specify which team and Unit-no need to mention specifically the names of colleagues)	☒

Staff in the web team can access the personal data of all registered users. Course project managers can view the personal data of registered users who are enrolled in their courses.
FRA staff in the web team have access to administration parts of the platform and can view participants activity in the courses. Course managers can view which users are enrolled in their courses.

Recipients **outside** FRA:
(please provide a generic/functional mailbox) ☒

Selected staff members of the contractor Eworx
FRA@eworx-intl.com

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.

[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.

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 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"?

The user can request deletion of their account at any time. This request will be handled by the web team within 2 weeks of the date of the request.

Due to the specific features of the Learning Management System (forum posts and ongoing courses), the user record is not deleted from the Maria DB database (Maria DB is the Open Source database which is used to store all Moodle data and is installed on FRA's servers together with the Moodle software). When a user's data is deleted, any forum posts are blanked and replaced with a sentence stating that the post has been removed, their username is changed to a combination of their email address and

a timestamp from when the account was deleted and an encrypted version of the username is stored as the email address. So if username is **username**, and email address is **email@institution.com**, the username field in the data table now reads:

- email@instution.com.1678115634

With regards to the deletion of Data Requests, Moodle deliberately **does not** remove deletion requests. These are kept to serve as a paper trail that the deletion was actually processed and this is allowed under GDPR. It falls under the basis of Legal Obligation as the record is required to prove that you received, and acted upon the request in accordance with the legislation. Related to this we do not anonymise all data in the user record because it is required to identify the user that the request has been processed for.
This is the standard behaviour of Moodle software and has been implemented to balance the need to retain certain data for courses eg a course participant starts a new thread in a form and the requirements for data retention and anonymisation. The retention of the email address in the username is retained on the basis of "legal obligation", i.e. if it wasn't it would not be possible to report on if a deletion request has been actioned.

Users who have been inactive for more than 12 months will be deleted automatically. After 12 months of inactivity, an email will be sent to the user to ask them to log in or their account will be deleted in 2 weeks.

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	☒

Other (please specify):

The e-learning platform is hosted in the servers of FRA's external web hosting contractor. The data is stored in the EU and not transferred outside of the EU.

FRA undertakes to ensure security updates to the software and hosting environment take place in a timely manner.

The consortium has security policies in place to ensure the physical and logical security for the infrastructure it operates.

FRA
EUROPEAN UNION AGENCY
FOR FUNDAMENTAL RIGHTS

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 webfeedback@fra.europa.eu. *We will reply as per standard deadlines and procedures in FRA's data protection implementing rules.*

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