DATA PROTECTION NOTICE
EUAA Learning Management System

1. Introduction

The European Union Agency for Asylum (hereinafter ‘the EUAA’ or ‘the Agency’) is committed to protecting your privacy. The EUAA collects and further processes personal data pursuant to Regulation (EU) 2018/17251 (hereinafter ‘the EUDPR’).

This Data Protection Notice explains inter alia the reasons for the processing of your personal data, the way we collect, handle, and ensure protection of your personal data and what rights you have in relation to your personal data. It also specifies the contact details of the responsible Data Controller with whom you may exercise your rights, as well as of the Data Protection Officer (DPO) and the European Data Protection Supervisor (EDPS) to which you may have recourse as well to exercise the said rights.

2. Why and how do we process your personal data?

The EUAA Learning Management System (hereinafter ‘the LMS’) is an online training platform accessible from the Agency’s Intranet, which is used to deliver interactive modules covering the entire field of international protection to EUAA personnel (i.e., staff members, temporary agency workers / interim workers and remunerated external experts) and to personnel working in the asylum and reception administrations of EU+ Countries (i.e., case officers, managers of asylum units, reception officers, Country of Origin (COI) researchers and policy officers), amongst others. The training provided via the LMS includes sessions organised at the EUAA or at the national level, consisting of interactive e-Learning modules covering the core aspects of international protection procedures.

For trainers, personal data are either collected directly by the Agency (where the EUAA assigns in-house trainers based on their availability and expertise) or provided to the Agency by Training National Contact Points (TNCPs)2 both in the context of a deployment procedure, for sessions organised by the EUAA, and in the context of national training sessions. This information is required to register trainers on the LMS, set up their personal profiles on the platform and decide on the appropriate trainer(s) for specific session(s).

For learners, personal data are provided to the Agency by TNCPs using a dedicated registration form. This information is required to register learners on the LMS, set up their personal profiles on the platform and enrol them in their chosen courses. It is also required to deliver and evaluate EUAA training activities via the platform. In addition, learners’ personal data contained in module evaluations are processed by the Agency for reporting purposes, with a view to increasing the quality of the


2. Where references to Training National Contact Points (TNCPs) are included, that definition needs to be extended to other national administration officials, communicating with the Agency on behalf of or in coordination with the TNCP(s).
modules delivered. To execute such tasks, selected EUAA personnel have access to learners’ personal data stored in the registration forms and on the LMS platform.

When using the LMS platform, personal data are processed in the following manner:

- User data are collected via the LMS internal tools for the purpose of providing learners/trainers access to EUAA modules, managing the LMS and the generation of reports (e.g., LMS user enrolment report, LMS activity completion report, trainers report, etc.).
- Learner experience data which are related to real-time spent on different sections of the LMS, and data related to online interactions on the system are collected automatically via the LMS. Learner experience data are also collected directly in the LMS live session and are accessible by the assigned trainer(s) to monitor learners’ progress during the online phase of the module. With the help of EUAA administrators, this helps to identify and measure the impact of the engagement of learner(s) at risk of dropping out to enable tutoring intervention in order to facilitate the completion of their training, and to improve the overall quality of the service. These data are also collected to mark learners’ responses automatically during quiz-based assessment sessions. In this case, scores are automatically attributed to learners based on the number of correct answers they provide, and the results are available online to the concerned users.
- (Anonymised) feedback information about the LMS is collected from learners and trainers via the feedback form plugin (SurveyPro) for purposes related to the (re)design of the curriculum (e.g., for the EUAA Annual Training Report).

3. On what legal ground(s) do we process your personal data?

We process personal data on the basis of Article 2(1) point (d) of Regulation (EU) 2021/2303 (hereinafter ‘the EUAA Regulation’), which provides that the Agency’s tasks include “assist[ing] Member States as regards training and, where appropriate, provid[ing] training to Member States’ experts from all national administrations, courts and tribunals, and national authorities responsible for asylum matters, including through the development of a European asylum curriculum”.

More specifically, paragraphs 1 to 4 of Article 8 of the EUAA Regulation provide, inter alia, that the Agency “shall establish, develop and review training for members of its own staff and members of the staff of relevant administrations, courts and tribunals, and of national authorities responsible for asylum and reception” and “shall develop a European asylum curriculum [...] to promote best practices and high standards in the implementation of Union law on asylum”, offering such high quality training “with a view to ensuring greater convergence of administrative methods, decisions and legal practices, while fully respecting the independence of national courts and tribunals”.

Consequently, the relevant processing operation is lawful under Article 5(1) point (a) of the EUDPR given that it is necessary for the performance of the tasks that the Agency has been vested with by virtue of its mandate.

---

3. For further information, please consult Section 12.1 of the EUAA Training Quality Assurance Framework (2022).
To the extent that participation in the EUAA training activities taking place in the context of the LMS may be voluntary, the processing of any personal data shared on this basis is also lawful under Article 5(1) point (d) of the EUDPR, as it is based on consent of the data subjects concerned.

4. Which personal data do we collect and further process?

The following (categories of) personal data may be processed (for learners and/or trainers):

1. Learners
   - Credentials
   - First name and surname
   - E-mail address
   - Organisation or institution of origin
   - Assessment of learners’ results and grades
   - Module completion status (i.e., enrolled, completed, withdrawn)
   - Learner experience data collected via the LMS internal tools:
     - Time spent on the LMS and in different sections of the training modules.
     - Interactions with online content and activities (e.g., LMS webpages, learning objects, quizzes, tests, forums and assignments).
     - Tracking of learning progress.

2. Trainers
   - Credentials
   - First name and surname
   - E-mail address
   - Organisation or institution of origin
   - Trainers’ feedback on learners’ assessment of results and grades
   - Learners’ (anonymised) feedback on trainers’ performance.

5. How long do we keep your personal data?

Learners’ personal data will be kept for a maximum of 40 years in accordance with Standard 8 of the Guidelines for External Quality Assurance Audits of Further Education Institutions and Further Education Centres issued by the Malta Further and Higher Education Authority (MFHEA), to meet the requirements of Maltese legislation for the accreditation of educational institutions.

Non-in-house trainers’ personal data will be stored for as long as trainers comply with the Trainers Pool selection criteria and are available for deployment as a trainer.

In-house trainers’ personal data are administrative data stored by the Agency for as long as they work in the EUAA.
6. **How do we protect and safeguard your personal data?**

Personal data processed in the context of the LMS or data obtained for the purposes of registration in electronic format (e-mails, documents, etc.) are stored in Microsoft Azure and Microsoft 365 Services.

To protect personal data, the EUAA has put in place a number of technical and organisational measures as required under Article 33 of the EUDPR. Technical measures include 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.

For website security purposes and to ensure that the LMS remains available to all users, network traffic is monitored to identify unauthorised attempts to exploit or change information on this website or otherwise cause damage or conduct criminal activity. Anyone using this website is advised that if such monitoring reveals evidence of possible abuse or criminal activity, results of such activity might be provided to the appropriate authorities in line with the applicable rules.

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons posed by the processing, the following security measures are applied:

1. The pseudonymisation and encryption of the data.
2. Measures to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.
3. Measures to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.
4. A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
5. Measures to ensure personal data will solely be processed by authorised personnel who are:
   a. granted access to the personal data on a need-to-know basis.
   b. familiar with the obligations stemming from the applicable data protection rules.
   c. regularly trained in the care, protection and handling of personal data.
   d. authorised to process the personal data; and
   e. subject to a duty of confidentiality (either as a statutory or as a contractual obligation).
6. Additional particular security controls: The Information and Communications Technology Unit (ICTU) of the EUAA has implemented and maintains the following security controls for user data, consistent with industry best practices, including:
   a. Controls, Policies & Procedures: Appropriate technical and administrative controls, and organisational policies and procedures.
   b. Named person in the role as a dedicated Information Security Officer (ISO) with focus on security in all areas of the EUAA business.
   c. Logging: System and application logging where technically possible, whereas the EUAA ICTU retains logs and verifies such logs periodically for completeness.
d. Malicious code and/or software: Malware prevention software (e.g., antivirus) is implemented on the technical infrastructure where applicable; XDR solution (Cortex) is used on all LMS Virtual machines.

e. Traffic inspection: Vulnerability exploit inspection is implemented on the technical infrastructure where applicable.

7. System Security: System and IT security controls are applied by the ICTU, consistent with industry best practices, including:

a. A high-level infrastructure diagram, which can be provided upon request.

b. A mix of industry standard software firewalls to dynamically limit external and internal traffic between the Agency’s services.

c. A program for evaluating security patches and implementing patches using a formal change process within defined time-limits.

d. Ad-hoc penetration testing by an independent third party, with a detailed written report issued by such third party and provided upon request.

e. Documentation of identified vulnerabilities ranked based on risk severity and corrective action according to such rank.

f. Password policy controls implemented to protect data, including complexity requirements and multi factor authentication where available.

Who has access to your personal data and to whom are they disclosed?

The following (categories of) recipients may have access to personal data related to learners/trainers identified above:

- Trainers;
- Learners in the same training module(s);
- Other users (i.e., trainers or learners) participating in discussion forums, personal/group messaging tools, chat rooms or with access to list(s) of participant(s) for different module(s);
- Authorised EUAA personnel acting as LMS administrators with access rights;
- External contractors (ALTIA CONSULTORES S.A) based in the EU/EEA providing LMS-related services with access rights (i.e., Helpdesk and Maintenance Services);
- TNCPs.

Do we transfer any of your personal data to third countries or international organisations (outside the EU/EEA)?

To the extent that users of the LMS (i.e., trainers or learners) may come from (international) organisations5 and/or third country partners under EUAA Roadmaps6, this processing activity may entail transfers of personal data to (international) organisations or third countries.

---

5. Namely, the United Nations High Commissioner for Refugees (UNHCR) (see applicable privacy policy here), the International Organisation for Migration (IOM) (see applicable privacy policy here), the Council of Europe (CoE) (see applicable privacy notice here), the International Centre for Migration Policy Development (ICMPD) (see applicable privacy notice here), the Intergovernmental Consultations on Migration, Asylum and Refugees (IGC) and the General Directors of Immigration Services Conference (GDISC).

For this purpose, in the absence of appropriate safeguards in place, the explicit and informed consent of the data subject(s) concerned is exceptionally sought for the international transfers of their personal data, pursuant to the derogation foreseen in Article 50(1) point (a) of the EUDPR.

9. Does this processing involve automated decision-making, including profiling?

This processing activity does not involve automated decision-making, nor profiling.

10. What are your rights and how can you exercise them?

According to the EUDPR, you are entitled to access your personal data and to rectify them in case the data are inaccurate or incomplete. If your personal data are no longer needed by the EUAA or if the processing operation is unlawful, you have the right to erase your data. Under certain circumstances, such as if you contest the accuracy of the processed data or if you are not sure if your data are lawfully processed, you may ask the Data Controller to restrict the data processing. You may also object, on compelling legitimate grounds, to the processing of data relating to you. Additionally, you have the right to data portability which allows you to obtain the data that the Data Controller holds on you and to transfer them from one Data Controller to another. Where relevant and technically feasible, the EUAA will do this work for you.

If you wish to exercise your rights, please contact the Data Controller, i.e., Head of Training and Learning Technologies Sector by sending an e-mail to registrar@euaa.europa.eu.

You may always submit queries, remarks or complaints relating to the processing of your personal data to the Data Protection Officer (DPO) of the EUAA using the following e-mail address: dpo@euaa.europa.eu.

In case of conflict, complaints can be addressed to the European Data Protection Supervisor (EDPS) using the following e-mail address: edps@europa.eu.