EUROPEAN EDUCATION AND CULTURE
EXECUTIVE AGENCY (EACEA)

RECORD OF PERSONAL DATA PROCESSING

Art. 31 REGULATION (EU) 2018/1725 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (henceforth the "Regulation")

Record nº	2022-06

In accordance with Article 31 of Regulation (EU) 2018/1725, individuals whose personal data are processed by the Agency in any context whatsoever are to be protected with regard to the processing of personal data and the Agency has to keep records of their processing operations.

This record covers two aspects:
1. Mandatory records under Article 31 of the Regulation (recommendation: make the header and part 1 publicly available)
2. Compliance check and risk screening (initial; part 2 is internal only to the Agency, not published)

The ground for the record is (tick the relevant one):

☒ Regularization of a data processing operation already carried out
☐ Record of a new data processing operation prior to its implementation
☐ Change of a data processing operation.

Electronic Platform for Adult Learning in Europe ('EPALE')	
1	**Last update of this record (where applicable)**
	01/07/2022
2	**Short description of the processing**

	EPALE is a European, multilingual, open membership community of adult learning professionals, including adult educators and trainers, guidance and support staff, researchers and academics, and policy makers. It provides a platform where EPALE registrants can communicate and collaborate. EPALE is funded by the Erasmus+ programme. It is part of the European Union's strategy to promote more and better learning opportunities for all adults. EPALE does this by supporting and strengthening the adult learning practitioners. It enables members to connect with and learn from colleagues throughout Europe, through its blogs, forums, partner-finding tools, complemented with physical gatherings. EPALE addresses all adult education stakeholders in Europe, in particular local, regional, national and European policymakers, staff and organisations involved in providing adult learning, as well as researchers, students in the field and the media. It is managed by a Central Support Service (CSS) at European level, underpinned, at national level, by National Support Services (NSS) in the Erasmus+ Programme Countries participating in EPALE. Currently, there are 37 NSSs operating. Personal data is processed in order to allow interested individuals to create user accounts and consequently use the different functionalities of the platform (e.g., upload or download information/documents, make announcements, participate in networking activities, attend online events, subscribe to newsletters, share user experience, add details to their profiles, and find partners). Personal data of registered users is also processed by the EPALE mobile application.
Part 1 - Article 31 Record	
3	**Name of the Controller** **Unit(s) and/or function of person acting on behalf of the Controller**
	The controller is the European Education and Culture Executive Agency ('EACEA'). The person designated as being in charge of the processing operation: Head of Unit A.6: Platforms, Studies and Analysis, EACEA-EPLUS-EPALE@ec.europa.eu
4	**Contact details of the Data Protection Officer (DPO)**
	EACEA-data-protection@ec.europa.eu
5	**Name and contact details of joint controller** **(where applicable)**
	Not applicable
6	**Name and contact details of processor** **(where applicable)**

	The EPALE Central Support Service (CSS) is provided by Tremend Software Consulting Srl based in Romania and Lai-Momo Società Cooperativa Sociale based in Italy. Contact details: helpdesk@epale-support.eu DG DIGIT provides the IT hosting service for the EPALE platform. Contact details: EC-EUROPA-IT-PLATFORM@ec.europa.eu
7	**Purpose of the processing**
	The purpose of the processing of personal data is to operate the EPALE platform and mobile application and provide related services. The personal data is processed in order to implement the activities of the Central Support Service (CSS), including: - Set up and manage the users' accounts on both EPALE platform and mobile application. - Protect the website against malicious activities. - Assure quality of the online content (e.g., monitoring and validation of publications on the EPALE platform). - Organise and manage online events (including live streaming and/or recording, if needed) and/or physical events. - Inform users about EPALE activities through a newsletter (when users register to EPALE they can also sign up for the EPALE newsletter). - Share user data with the National Support Services (NSS) to allow users to be contacted for national EPALE activities (e.g., national newsletters, participation in courses, seminars, workshops, conferences). The users have to give their consent upon registration by selecting to allow their National Support Service to contact them via email for dissemination of informative and promotional materials on EPALE. - Allow interaction and networking among the EPALE community members through the internal messaging system that does not allow sharing of sensitive data. - Identify new user needs and improve the quality/functioning of the EPALE platform. - Perform statistical analyses.
8	**Description of the categories of data subjects**
	☐ Agency staff (Contractual and temporary staff in active position) ☐ Visitors to the Agency ☐ Contractors providing goods or services ☐ Applicants ☐ Relatives of the data subject ☐ Complainants, correspondents and enquirers ☐ Witnesses ☐ Beneficiaries ☐ External experts

	☐ Contractors ☒ Other, please specify**:** Users of the EPALE platform and mobile application: anyone can register on the platform and use the app, but they mostly target adult education stakeholders and communities in Europe, in particular local, regional, national and European policymakers, staff and organisations involved in providing adult learning, as well as researchers, students in the field and the media.
9	**Description of personal data categories**
	a) General categories of personal data: ☐ in the form of personal identification numbers ☒ concerning the physical characteristics of persons as well as the image, voice or fingerprints (optional, see details in section d) below) ☒ concerning the data subject's private sphere (optional, see details in section d) below) ☐ concerning pay, allowances and bank accounts ☐ concerning recruitment and contracts ☐ concerning the data subject's family ☒ concerning the data subject's career (optional, see details in section d) below) ☐ concerning leave and absences ☐ concerning missions and journeys ☐ concerning social security and pensions ☐ concerning expenses and medical benefits ☒ concerning telephone numbers and communications (optional, see details in section d) below) ☒ concerning names and addresses, including e-mail addresses and country (mandatory) ☒ Other, please specify: additional personal data can be voluntarily submitted by the users themselves during events, in the blog function, the partner search tool, and/or in the public, private or closed groups of the EPALE website, which are created on the platform to share ideas and opinions, to exchange good practices, or to network. ***b) Categories of personal data processing likely to present <u>specific risks:</u>*** ☐ data relating to suspected offences, offences, criminal convictions or security measures ☐ data being used to evaluate personal aspects of the data subject (ability, efficiency, conduct)

	c) Categories of personal data whose processing is <u>prohibited</u>, with exceptions (art. 10): ☐ revealing racial or ethnic origin ☐ revealing political opinions ☐ revealing religious or philosophical beliefs ☐ revealing trade-union membership ☐ concerning health ☐ genetic data, biometric data for the purpose of uniquely identifying a natural person ☐ concerning sex life or sexual orientation ***d) Specify any additional data or explanatory information on the data being processed, if any:*** **Optional data at user profile level** - Related thematic areas of interest - Features of interest on the site (e.g. partner search) - Online activity - Photo - Gender - Phone number - City - Short bio - Job title - Organisation - Occupation / role - Social media profiles - Language(s) used **Optional personal data voluntarily submitted by the users themselves in the collaborative sections and posts (e.g., Blogs, News, etc.)** - Comments in discussions - Comments or educational materials posted in the Resources centre - Comments or educational materials posted in the National Support Services (NSS) closed group (accessible only to NSSs and the Central Support Service) and other private and public groups - Files, images, videos and blog posts - Messages in the Partner search tool **Optional personal data submitted on voluntary basis during online events** - Voice and images of participants who voluntarily choose to turn on their microphone and camera in order to participate in the discussions
10	**Retention time (time limit for keeping the personal data)**
	Indicate the <u>period of storage</u>:

	- Traffic data, data logs and server data will be kept for 3 years from 31 October 2019. - Contact details: 2 years after the user's last login his/her profile may be deactivated. One month before this deadline a notification is sent to this user to inform him/her about the upcoming profile deactivation. The user can request to keep his/her account active. Otherwise his/her profile will be deactivated permanently. All information is then made anonymous. - Public and private groups: after 2 years of inactivity, a public and/or private group may be deactivated. One month before this deadline, a notification is sent to the group administrator to inform him/her about the upcoming deactivation. The group administrator can ask to keep the group active, otherwise it will be deactivated permanently. After deactivation no data of the respective group is visible on EPALE. - In case users ask for the deactivation of their profile or the profile is automatically deactivated, no data will be visible to other EPALE users. Data will be kept only in an anonymous form that does not allow for personal identification. If users with a deactivated profile want to continue using the platform, they will need to register again. The data remains solely for research and monitoring purposes at the disposal of EACEA, the European Commission, the NSSs and researchers specifically allowed by the data controller. - Data relating to the registration process of online events will be kept for 6 months after its closure. Information identifying the data subjects can be kept for a longer period for historical, statistical or scientific purposes with the appropriate safeguards in place. Recordings from online workshops will be kept online for 2 years before being deleted. - Personal data of speakers, including recordings from web-streamed plenary sessions, will be kept online for 4 years before being deleted. This will allow the general public and any interested individuals to freely access and/or watch again the relevant content. - Blog posts, educational materials posted in the Resource centre and files, images, videos submitted in the communities of practice will be kept for a maximum of 5 years on the EPALE platform. - Messages and comments by users, alongside files, images, videos and blog posts submitted in the collaborative spaces and closed groups, will be kept for a maximum of 5 years on the EPALE platform. These also include messages and personal data in the Partnership search tool - News and events published on the website will be kept for a maximum of 2 years on the EPALE platform. **Is any further processing for historical, statistical or scientific purposes envisaged?** ☐ yes ☒ no Anonymised data will be used for the following purposes: - Analysis of the information accessed and produced on the site and through the mobile application in order to improve the quality of the services provided. - Review of thematic areas and features of interest in order to provide more accurate information related to adult learning. **If yes, indicate the further retention time:** If the answer is yes, please go to point 5 Part 2, Storage and Security for technical safeguards.
11	**Recipients of the data**
	– Authorised staff of EACEA and European Commission, Directorate-General for Education, Youth, Sport and Culture (DG EAC) and Directorate-General for Employment, Social Affairs and Inclusion (DG EMPL).

	– Authorised staff of Tremend Software Consulting Srl and Lai-Momo Società Cooperative Sociale. – EPALE National Support Services (NSS), who are in charge of promoting EPALE to the local and national stakeholders and keeping contact with them. Each NSS receives the personal data of the users of its respective country, if the users agreed with this upon registration. – Registered users: information made public by the registered users' participating in the closed groups, blogs, etc. are visible to the other participants in these groups. – The general public for recordings and/or live steaming of events on the EPALE platform. In addition, data may be disclosed to public authorities, and processed by these authorities in compliance with the applicable data protection rules according to the purpose of the processing, including inter alia: – The European Court of Justice or a national judge as well as the lawyers and the agents of the parties in case of a legal procedure; – The competent Appointing Authority in case of a request or a complaint lodged under Articles 90 of the Staff Regulations; – OLAF in case of an investigation conducted in application of Regulation (EC) No 1073/1999; – The Internal Audit Service of the Commission within the scope of the tasks entrusted by Article 118 of the Financial Regulation and by Article 49 of the Regulation (EC) No 1653/2004; – IDOC in line with Commission Decision C(2019)4231 of 12 June 2019 laying down general implementing provisions on the conduct of administrative inquiries and disciplinary proceedings and Commission Decision (EU) 2019/165 of 1 February 2019 laying down internal rules concerning the provision of information to data subjects and the restriction of certain of their data protection rights in the context of administrative inquiries, pre-disciplinary, disciplinary and suspension proceedings; – The Court of Auditors within the tasks entrusted to it by Article 287 of the Treaty on the Functioning of the European Union and Article 20, paragraph 5 of Regulation (EC) No 58/2003; – The European Ombudsman within the scope of the tasks entrusted to it by Article 228 of the Treaty on the Functioning of the European Union; – The European Public Prosecutor's Office within the scope of Article 4 of Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office.
12	**Are there any transfers of personal data to third countries or international organisations? If so, to which ones and with which safeguards?**
	NSS: The personal data of registered users is shared with certain NSSs, which are based outside the EU/EEA in the following third countries: Albania, Bosnia and Herzegovina, Montenegro, North Macedonia, Serbia and Turkey, if the user gave his/her explicit consent upon registration to share his/her data with the local NSS under article 50(1)(a) of the Regulation. Please note that for these countries, the EU has not adopted an adequacy decision pursuant to Article 47 of Regulation (EU) 2018/1725, certifying that your personal data, once transferred, will benefit from an adequate level of protection in the third country of destination. Therefore, the level of protection of your personal data transferred will depend on the law or practice of that third country and, as a result, your rights as regards data protection might not be equivalent to those in and EU/EEA country or a country with an adequacy decision. The NSS is bound by data protection clauses, in particular in relation to lawfulness of processing and technical and organisational security obligations, under a grant agreement signed with the Agency. The users may request to obtain a copy of these clauses by contacting the controller indicated in section 3 above.

	The complete and updated list of those countries, as well as of all NSSs, is available in the dedicated page (https://ec.europa.eu/epale/en/nss). Registered users: As mentioned under section 11, information made public by the registered users can be seen by other users, some of them could be based outside the EU/EEA. When explicit consent does not apply, the following is applicable: The transfer of personal data outside EU/EEA is necessary for important reasons of public interest and is based on Article 50(1)(d) of the Regulation as recognised in the following Union law: • Article 14 of the Charter of Fundamental Rights of the European Union, • Article 26 of the Universal Declaration of Human Rights, • Article 11 of the Treaty of the European Union, • Article 15 of the Treaty on the Functioning of the EU. As stated in the Erasmus+ Programme funding this process, the European Commission highlighted in its communication of 14 November 2017 entitled 'Strengthening European identity through education and culture' the pivotal role that education plays in promoting active citizenship (Recital no 21 of the Erasmus+ Regulation (EU) 2021/817).
13	**General description of the technical and organisational security measures**
	The EPALE servers are hosted on Amazon Web Services in European Data Centres. DG DIGIT manages the cloud infrastructure in a highly secured environment. Only authorised personnel have access to the storage media at the Data Centres and the sites are subject to strict physical security. DG DIGIT ensures the security of the IT hosting service in conformance with the Commission's Information Security Policy and Framework and DIGIT's complementary Information Security Policy Framework. See also Commission Decision C(2006)3602 of 16 August 2006 concerning the "Security of information systems used by the European Commission" and "Implementing rules of 16.8.2006 concerning the security of information systems used by the European Commission". Personal data is only communicated using HTTPS encryption. No personal data is transported using storage media. Additionally any database backups are sanitised and user information is anonymised. DG DIGIT provides to the EPALE Central Support Service technical team anonymised database dumps. The database back-up service is behind a password-protected system. The anonymised database is used for platform development, All development servers are utilising strong password access and where required VPN encrypted connection, and in many cases biometric access. Online platforms used as part of the project use password protected access, permission systems to prevent anyone but those authorised any access to personal data. No database back-ups containing personal data is stored on any removable storage devices. Only a limited number of named individuals (maximum 3) from the development team in Tremend Consulting have access to the highest level of permission in information systems, and where personal data is stored in a document or database, it is only on a needs-access basis. By ensuring that the lowest number of users have access to the information systems, the data processor ensures the lowest level of risk. Data in transit is encrypted via SSL/TLS, management access and data transfers on platforms are done securely.

14	**Information to data subjects / Privacy Statement**
	https://epale.ec.europa.eu/en/privacy-statement