EUROPEAN COMMISSION
European Education and Culture Executive Agency

# 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** 02-2022

*In accordance with Article 31 of Regulation 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*
☐ *Migration from notification to record.*

## Development of the European Digital Education Hub

| | |
|---|---|
| 1 | **Last update of this record (where applicable)** |
| | First version of this record was from 17/05/2022 |
| 2 | **Short description of the processing** |
| | The European Digital Education Hub is an initiative of the European Commission, funded by the Erasmus+ programme (2021-2027) and operated by a consortium of organisations, under a service contract with the European Education and Culture Executive Agency (EACEA). The Community of Practice of the European Digital Education Hub promotes networking, knowledge building, peer learning, exchange, and collaboration among stakeholders in the field of digital education. The online Community is hosted and engages in online activities on the European Commission's Microsoft 365 environment. Data processing is necessary to register interested individuals as members of the European Digital Education Hub Community, to give registered members access to the Microsoft (MS) Teams platform, and to allow them to engage in the Community activities conducted on the MS Teams platform. |

| | |
|---|---|
| | **Part 1 - Record** |
| 3 | **Name of the Controller<br>Unit(s) and/or function of person acting on behalf of the Controller** |
| | European Education and Culture Executive Agency (EACEA)<br>Person designated as being in charge of the processing operation: Head of Unit A.6 Platforms, Studies and Analysis<br>EACEA-DIGITAL-EDUCATION-HUB@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<br>(where applicable)** |
| | N/A |
| 6 | **Name and contact details of processor<br>(where applicable)** |
| | The following contractors of EACEA act as data processors:<br>1) German Academic Exchange Service (DAAD)<br>Kennedyallee 50<br>53175 Bonn, Germany<br>DAAD's Data Protection Officer is:<br>Dr Gregor Scheja<br>Scheja und Partner Rechtsanwälte mbB<br>Adenauerallee 136<br>53113 Bonn<br>Germany<br>Tel.: (+49) 0228-227 226 0<br>E-Mail: datenschutz@daad.de<br>Encrypted contact form: https://www.scheja-partner.de/en/contact/contact.html<br>https://www.scheja-partner.de/en/<br>2) Stifterverband für die Deutsche Wissenschaft (Stifterverband)<br>Barkhovenallee 1<br>45239 Essen, Germany<br>The DPO for Stifterverband is:<br>TÜV Informationstechnik GmbH<br>Unternehmensgruppe TÜV NORD<br>IT Security, Business Security & Privacy<br>Langemarckstraße 20<br>45141 Essen<br>Deutschland<br>T 0201 8999-623<br>F 0201 8999-666<br>E-Mail: privacyguard@tuvit.de<br>Contact point is Sebastian Kessler.<br>3) Vereniging van European Distance Teaching Universities (EADTU)<br>Parkweg 27, 5. Verdieping<br>6212 XN Maastricht, Netherlands |

secretariat@eadtu.eu

4) Unitatea Executiva pentru Finantarea Invatamantului Superior, a Cercetarii, Dezvoltarii si Inovarii (UEFISCDI)
Mendeleev Street 21-25
010362 Bucharest, Romania
protectiadatelor@uefiscdi.ro

5) EDEN Digital Learning Europe Mittetulundusühing (EDEN)
Kesklinna Linnaosa, Roosikrantsi tn 2-304 K
10119 Tallinn, Estonia
eden@eden-europe.eu

6) Educraftor Oy Ab
Aalto University Campus
Metallimiehenkuja 10
02150 Espoo, Finland
datasecurity@educraftor.com

7) Hasso-Plattner-Institut für Digital Engineering gGmbH HPI School of Design Thinking (HPI)
Prof. Dr. Helmert Strasse 2-3
14482 Potsdam, Germany

HPI's DPO is:
Dipl.-Inf. Christian Willems
Chief Information Security Officer | Technischer Leiter openHPI
Hasso-Plattner-Institut für Digital Engineering gGmbH
Campus Griebnitzsee | Universität Potsdam
Prof.-Dr.-Helmert-Straße 2 - 3 | 14482 Potsdam
Tel.: 0331 5509-513 | Fax: 0331 5509-325

7 **Purpose of the processing**

The purpose of the processing is **to build, support and nurture the Community of the European Digital Education Hub,** including to facilitate peer learning, mentoring, acceleration, exchange and knowledge-building activities, as well as providing information about the Community and its events (before, during and after).

The personal data collected is needed:

i. To register users as members of the Community, identify their areas of interest and grant them access to the European Commission's MS Teams platform.

ii. To contact interested members regarding calls for experts (e.g., to speak at an event), calls for participation or contribution (e.g., to take part in a working group "squad", take part in mentoring or acceleration activities, take part in design thinking workshops), which may also be part of a process of selecting candidates for activities with limited numbers of participants.

iii. To identify ambassadors who are willing to engage and support the Community members in activities.

iv. To match suitable mentors with mentees to sign a mentoring agreement as part of mentoring activities.

v. To engage members in the Community activities on the MS Teams platform and allow them to communicate, network and collaborate through posts, reactions and chats.

vi. To organise and manage online events (e.g. workshops, web-seminars, stakeholder meetings and round tables, online meetings, clinics, trainings, mentoring activities, peer-learning) through audio-visual conferencing and/or recording.

| | |
|---|---|
| | vii. To offer and manage other online learning activities (e.g., self-assessments as part of the mentoring; develop testbeds as part of the acceleration activities).<br>viii. To organise and manage physical events, including to contact the participants regarding organisational information (e.g., agenda, travel expenses, hotel, organising networking dinners and lunches in compliance with food allergies declared by participants); and in order to illustrate, promote or document the physical activities.<br>ix. To document conducted activities and showcase the best digital solutions by submitting digital artifacts (e.g., minutes, publications, reports, news items, case studies and/or other outputs) to the solution space on MS Teams and/or on the European Education Area Portal.<br>x. To allow for the analysis of members' feedback on Community activities (the main objective being quality monitoring and improvement).<br>xi. To monitor and evaluate the Community's growth by keeping track of the number of members, also in relation to represented sectors of education and training and members' geographical location for purposes of growing the Community in a balanced manner.<br>xii. Upon consent, to inform about European Digital Education Hub results and developments, upcoming events and/or other related initiatives of the European Commission through a dedicated newsletter.<br>xiii. To handle helpdesk inquiries and to provide technical support.<br>xiv. To be able to provide inclusive and accessible settings at physical events.<br><br>Individuals interested in joining the Community of the European Digital Education Hub must fill in an EUSurvey registration form (see full information about the processing of personal data under EUSurvey in data protection record No. DPR-EC-01488.1).<br><br>The framework of the MS Teams collaborations is defined in the data protection record for the European Commission's Microsoft 365 environment (reference No. DPR-EC-04966.4).<br>The personal data of registered members will not be used for any automated decision-making including profiling. |
| 8 | **Description of the categories of data subjects** |
| | Whose personal data are being processed?<br><br>□ Agency staff (Contractual and temporary staff in active position)<br>□ Visitors to the Agency<br>□ Contractors providing goods or services<br>□ Applicants<br>□ Relatives of the data subject<br>□ Complainants, correspondents and enquirers<br>□ Witnesses<br>□ Beneficiaries<br>□ External experts<br>□ Contractors<br>☒ Other, please specify: All registered members of the Community of the European Digital Education Hub on the MS Teams platform (e.g. preschool/school/vocational education and training (VET)/adult learning/higher education teachers or leadership, facilitators (non-formal education), policy makers, researchers, Education technology (EdTech) entrepreneur/developer, etc. at EU, national and regional/local level). |
| 9 | **Description of personal data categories** |
| | ***a) 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)

Community members may voluntarily submit or share their image and voice during online events, in videoconferencing, audio calls, video recordings and/or podcasts. They may decide to voluntarily share their picture(s) in public or private channels of the MS Teams platform, e.g., as part of photo contests, news items, and event announcements. They may also voluntarily share their experiences, opinions, pictures and quotes for articles to be published within the Hub and on the EEA portal.
Optional: Speakers and participants who take part in physical events may have recordings, live-streaming and photographs of themselves taken during the events, to be used for promotion on the Hub, the EEA Portal and the EUDigitalEducation Twitter account owned by DG EAC.

Data subjects can publish images of any other data subjects only with their explicit consent.

☒ concerning the data subject's private sphere (optional)

At registration, Community members may indicate their area(s) of interest in digital education.

After registration, Community members may provide information on their personal motivation to join the Community; they may post links and other resources that can belong to their private sphere, such as blogs or personal websites.

☒ concerning pay, allowances and bank accounts (optional)

To allow for remuneration of experts' work, their bank details will be asked for.

To be able to reimburse travel costs as well as accommodation and subsistence costs for physical Community events, bank details need to be collected from event participants.

☐ concerning recruitment and contracts

☐ concerning the data subject's family

☒ concerning the data subject's career

Mandatory: All Community members will share their current professional role and field of work when registering.

Optional: Individuals who are interested in registering as an "expert" can provide additional professional information, including on their experience and field(s) of expertise, as well as relevant achievements (e.g. job position, publication, course taught or a project managed).

In the context of calls for experts or calls for participation or contribution, providing information on the career of the Community members, their experiences with the topic of the event, their motivation/interest in the event and their intended follow-up actions after the event is mandatory as it serves as selection criteria.

In the context of self-assessment activities, providing information on current institutional affiliation, professional role and field of work is mandatory as it serves to guide the mentoring and training.

In the context of preparations for events, participants whose participation is confirmed may be asked to submit data regarding their experiences with the topic of the event and their intended follow-up actions after the event in EU survey questionnaires.

In the context of articles to be published on the Hub and the European Education Area (EEA) Portal, participants may voluntarily share experiences, opinions, pictures and quotes.

☐ concerning leave and absences

☒ concerning missions and journeys (optional)

To be able to reimburse travel, accommodation and subsistence costs for physical Community events, information on itineraries and travel receipts need to be collected from participants.

☐ concerning social security and pensions

☐ concerning expenses and medical benefits

☒ concerning telephone numbers and communications (optional)

Community members may share on a voluntary basis their telephone numbers with other members on the platform; they may also share their social media handles.

☒ concerning names and addresses, including email addresses (mandatory):

To register, users must submit their first name, last name, country of residence and e-mail address.

To request technical support, users must submit their first name, last name and e-mail address.

☒ Other (optional):

Community members may voluntarily share their food preferences (allergies, vegetarian options, halal, etc.) when registering for physical events where food is served.

Other (optional)

Community members may voluntarily share their special needs (such as accessible entrance to meeting rooms) when registering for physical events.

Other (optional)

Technical identifiers: To ask for assistance when facing technical problems with the platform, registered members may share screenshots providing information about their personal computers, internet connection and account settings, such as IP addresses and Microsoft account usernames.

***b) Categories of personal data processing likely to present specific risks:***

☐ 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 prohibited, with exceptions (art. 10):***

☐ revealing racial or ethnic origin

☐ revealing political opinions

☐ revealing religious or philosophical beliefs

☐ revealing trade-union membership

☒ concerning health *(see above)*

☐ 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: _________***

10 **Retention time (time limit for keeping the personal data)**

**Indicate the period of storage**:

Personal data collected via **EUSurvey**
Personal data collected through EUSurvey and processed for registration purposes will be kept for 48 months.

Personal data collected on **MS Teams**
Identification data in MS Teams is stored for as long as the member's account is active. Service generated data (log files) are kept for up to six months. The retention period for content data in Office 365 and any personal data included therein is up to 180 days upon expiration/termination of the subscription. Diagnostic data is kept for up to five years. For more information, please refer to section 4 of data protection record No. DPR-EC-04966.4.

Personal data gathered for **physical events**
Data gathered for physical events (except regarding travel to/from the events, mentioned below) will be kept for six months. Live-streaming and audio-visual recordings of events will be kept for five years.

Personal data concerning pay, allowances and bank accounts and missions and journeys will be kept for 10 years in order to comply with the audit/accounting obligations of the responsible data processors.

**Is any further processing for historical, statistical or scientific purposes envisaged?**
☐ yes ☒ no

**If yes, indicate the further retention time:** N/A

If the answer is yes, please go to Part 2, Storage and Security for technical safeguards.

11 **Recipients of the data**

- Authorised staff of EACEA and the European Commission, in particular the Directorate-General for Education, Youth, Sport and Culture (DG EAC) and the Directorate-General for Informatics (DG DIGIT).
- Microsoft Teams and other recipients identified in data protection record No. DPR-EC-04966.4 concerning processing made via Microsoft Teams.
- Recipients identified in data protection record No. DPR-EC-01488.1 concerning processing made via EUSurvey.
- Authorised staff of the processors identified in section 6, and the following sub-processors: 1) European Schoolnet Partnership AISBL, Belgium, 2) Learning Planet Institute (CRI), France; 3) Knowledge Innovation Centre Ltd., Malta; and 4) Open Evidence SL, Spain.
- Registered members of the Community who have access to personal data available or shared on a voluntary basis in the MS Teams channels.

Personal data can be published on the EUDigitalEducation Twitter account owned by DG EAC.

Personal data made public by registered Community members in the MS Teams channels can be seen by other users. Some of them could be based outside the EU or the European Economic Area. The general public will also have access to any workshop content/outputs (including images) published by EACEA and/or the European Commission via the Internet, including on the European Education Area Portal.

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?**

There are no direct transfers of personal data to third countries. However, limited personal data from MS Teams might be transferred to the United States as foreseen in section 6 of data protection record No. DPR-EC-04966.4. Any such transfers are subject to appropriate safeguards, namely the signature of standard data protection clauses adopted by the European Commission.

13 **General description of the technical and organisational security measures**

**EUSurvey**

The EUSurvey data is stored on European Commission servers managed by DG DIGIT in line with the technical security provisions laid down in the Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission, its subsequent versions, its implementing rules (as adapted from time to time) and the corresponding security standards and guidelines, as well as the Commission Decision (EU, Euratom) 2015/443 of 13 March 2015 on the security in the Commission, its implementing rules and the corresponding security notices. These documents are available for consultation at the following address: https://ec.europa.eu/info/publications/security-standards-applying-all-european-commission-information-systems_en

The European Commission has implemented security measures to protect server hardware, software and the network from accidental or malicious manipulations and loss of data.

**MS Teams**

The technical and organisational security measures put in place for personal data collected and processed in MS Teams are defined in section 8 of data protection record DPR-EC-04966.4. The access to the MS Teams channels of the Community is limited to "owners" and "guests". Only specific teammates have access to private channels.

.

**Data controller**

The European Commission's IT systems used by EACEA abide by the Commission's security guidelines. The Agency must comply with Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission.

*a) Organisational measures*

A Corporate Local Informatics Security Officer (C-LISO) is in place. Its role includes supervising the Agency compliance with the relevant regulations, and the application of security measures recommend by DG DIGIT.

Organisational measures include appropriate access rights and access control. As a rule within the Agency, access to information systems, the file system or offices are subject to a series of authorisations where the person granting the access is different from the person

requesting or authorising the access - except in limited cases of delegation. The responsible person in the unit in charge of this action (processing operation of the current record) collects and places the documents on the secured drives of the Commission and all Agency staff are bound by a confidentiality obligation. The need to know principle applies in all cases. Documents received in paper format (e.g. invoices and interim/final reports) are stored in locked cupboards.
*b) Technical measures*
State of the art technical cybersecurity measures are implemented in the corporate systems, according to the security needs. Those measures are in constant evolution.

**Additional measures at the level of processors and sub-processors**
**1) Processors:**
To secure data, DAAD uses a set of different techniques. Data is being stored on secured fileservers inside DAAD or on certified cloud servers in the EU/EEA. Access to both types of servers is only provided to those who need to know. Additionally, external access to user accounts is secured via multi-factor authentication. In case personal data is being accessed by sub-processors of DAAD (e.g., for video production of Community testimonials for social media), contracts are signed which ensure that sub-processors secure data according to GDPR.

Stifterverband undertakes identical measures. Also, personal data is being stored on encrypted fileservers or certified cloud servers in the EU. Access is also on a need-to-know basis. User accounts are also secured on a multi-factor basis. In case data is accessed by partners of Stifterverband, a data processor agreement is concluded.

EADTU uses a set of different techniques in order to secure the personal data. Data is being stored on encrypted fileservers inside EADTU or on certified cloud servers in the European Economic Area countries. Access to both types of servers is only provided to those who need to know. Additionally, user accounts are secured via multi-factor authentication and encryption of the data.

UEFISCDI’s security measures include both procedural and technical procedures designed to protect, control and, overall, safeguard access to them. Data is kept secure by storing them only in databases (not file system) which is configured in such a way as:

- servers are stored on organization data centre premises,
- server access (to the database service) is granted via various network policies,
- user/admin credentials (to the database) are given only on a need-to-know basis and their access is limited to the areas that need access to,
- activity is logged to withstand audits.

EDEN uses certified cloud servers in the EU, with secure physical access only from the infrastructure provider. Access to the server is granted with 2-factor protection with randomly generated passwords.

To secure data, Educraftor uses a set of different techniques. Data is being stored on encrypted fileservers on certified cloud servers in the EU. Access to both types of servers is only provided to those who need to know. Additionally, user accounts are secured via multi-factor authentication. In case data is being accessed by partners of Educraftor, no personal data is shared.

HPI D-School uses a set of different techniques to secure data. Data is being stored on encrypted fileservers inside HPI or on certified cloud servers inside HPI, Germany. Access to both types of servers is only provided to those who need to know. Additionally, user accounts are secured via multi-factor authentication. In case data is being accessed by sub-processors of HPI, contracts are signed which ensure that sub-processors secure data according to GDPR.

**2) Sub-processors:**
European Schoolnet Partnership AISBL (EUN) has implemented and continues to maintain appropriate state-of-the-art technical and management measures to keep personal data

| | |
|---|---|
| | secure and safe from loss, damage, corruption or deletion. The Technical Team has put in place an Acceptable Use Policy applying to all its staff (employees, contractors, in-house consultants, temporary staff) governing their use of the technical infrastructure and equipment of the Office. This policy is an important element in safeguarding and protecting the technical infrastructure. In accordance with its obligations under the GDPR, EUN maintains a data breach log under the control of the EUN Compliance Officer. Data breaches are reported without delay to the Technical Team and the Data Protection Officer who investigate and decide whether the Data Protection Authorities and the affected data subjects, must be notified under the GDPR and advise the Executive Director accordingly. The circumstances surrounding the breach are also investigated to prevent future breaches.<br>Learning Planet Institute (CRI)'s data stored on local computers are encrypted by default. They are only accessible if one knows the key to decrypt the hard drive and one knows the credentials to log in to the user account. The Heroku cloud is password-protected; access to data is restricted to some members only.<br>Knowledge Innovation Centre Ltd. (KIC)<br>In order to secure data, KIC uses a set of different techniques. Data is being stored on encrypted fileservers inside KIC or on certified cloud servers inside the EU. Access to both types of servers is only provided to those who need to know. Additionally, user accounts are secured via multi-factor authentication. All services used by KIC are processed in the cloud, using the zoho.eu suite of services, which are wholly located in the EU with datacentres in Amsterdam and Dublin. The GDPR statement of the company is available here: GDPR \| Zoho.<br>Open Evidence SL<br>To secure data, Open Evidence uses a set of different techniques. Data is being stored on encrypted fileservers inside Open Evidence or on certified cloud servers in the EU. Access to both types of servers is only provided to those who need to know. Additionally, user accounts are secured via multi-factor authentication. In case data is being accessed by sub-processors of Open Evidence, contracts are signed to ensure that sub-processors secure data according to GDPR. |
| 14 | **Information to data subjects / Privacy Statement** |
| | The data protection notice is attached to the EUSurvey registration form available on the General MS Teams channel of the Community under "Files" and also in the Hub instructions manual. |