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)**
	The first version of this record is from 17/05/2022. The record was updated on 25/11/2022.
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 and occasionally onsite.

Part 1 - Record	
3	**Name of the Controller** **Unit(s) and/or function of person acting on behalf of the Controller**
	European Education and Culture Executive Agency (EACEA) Person designated as being in charge of the processing operation: Head of Unit A.6 Platforms, Studies and Analysis 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 (where applicable)**
	N/A
6	**Name and contact details of processor (where applicable)**
	The following contractors of EACEA act as data processors: 1) German Academic Exchange Service (DAAD) Kennedyallee 50 53175 Bonn, Germany DAAD's Data Protection Officer is: Dr Gregor Scheja Scheja und Partner Rechtsanwälte mbB Adenauerallee 136 53113 Bonn Germany Tel.: (+49) 0228-227 226 0 E-Mail: datenschutz@daad.de Encrypted contact form: https://www.scheja-partner.de/en/contact/contact.html https://www.scheja-partner.de/en/ 2) Stifterverband für die Deutsche Wissenschaft (Stifterverband) Baedekerstraße 1 45128 Essen, Germany The DPO for Stifterverband is: TÜV Informationstechnik GmbH Unternehmensgruppe TÜV NORD IT Security, Business Security & Privacy Langemarckstraße 20 45141 Essen Deutschland T 0201 8999-623 F 0201 8999-666 E-Mail: privacyguard@tuvit.de Contact point is Sebastian Kessler.

	3) Vereniging van European Distance Teaching Universities (EADTU) Parkweg 27, 5. Verdieping 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: Chief Information Security Officer (CISO) | Informationssicherheitsbeauftragter Prof. Dr. Christian Dörr Hasso-Plattner-Institut für Digital Engineering gGmbH Campus Griebnitzsee | Universität Potsdam Prof.-Dr.-Helmert-Straße 2 - 3 | 14482 Potsdam ciso@hpi.de Phone: +49-331-5509 225 DG CNECT for the use of Newsroom
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 European Digital Education Hub 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 contact members by email within one month of their registration, reminding them of upcoming activities which may be interesting for them.

iv. To identify ambassadors who are willing to engage and support the Community members in activities.
v. To match suitable mentors with mentees and sign a mentoring agreement as part of mentoring activities.
vi. To engage members in the Community activities on the MS Teams platform and allow them to communicate, network and collaborate through posts, reactions, tags and chats.
vii. To award "badges" to active Community members through the Europass platform.
viii. 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.
ix. 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).
x. 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 preferences/allergies declared by participants), to be able to provide inclusive and accessible settings at physical events, and in order to illustrate, promote or document the physical activities.
xi. To document conducted activities and showcase the best digital solutions by submitting digital artifacts (e.g., minutes, publications, reports, news items, interviews, case studies, interviews, videos and/or other outputs) to the solution space on MS Teams and/or on the European Education Area Portal.
xii. To allow for the analysis of members' feedback on Community activities (the main objective being quality monitoring and improvement).
xiii. 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.
xiv. Upon consent, to present members, information about European Digital Education Hub results and developments, upcoming events and/or other related initiatives of the European Commission through a dedicated newsletter.
xv. To handle helpdesk inquiries and to provide technical support.
xvi. To select members of the Higher Education Interoperability Workgroups.
xvii. To be able to prove that participants have attended certain online and physical events.
xviii. To follow up with members of squads for additional output needed in order to finalise and publish the squad outputs.

Sometimes calls for participants, contributions and other calls may be promoted externally, leading to a situation where a non-Community member applies (even if there is an explicit disclaimer in each application form). In these cases, some personal data, including name, email address and call-specific questions related to the career of this non-Community applicant are processed. However, all applicants are informed that they need to register first as Community members, then to apply for the respective call.

Individuals interested in joining the Community of the European Digital Education Hub, as well as its Higher Education Interoperability Workgroups, 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 DPO Public register).

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).

The European Digital Education Hub newsletter is created and disseminated through the European Commission's corporate tool Newsroom, managed by DG CNECT (see data protection record No. DPR-EC-03928). Community members are free to subscribe to the

	newsletter when registering for the European Digital Education Hub. Subscriptions via Newsroom directly are also allowed and not limited to Community members. To illustrate or promote the activities/projects of the European institutions and the European Union, including of the European Digital Education Hub project, photographs and/or videos/films (including voices, first names, last names, and/or quotes/testimonials) may be archived in the European Union's online databases, accessible to the public free of charge online. Third parties having access to these databases may use the said photographs and/or videos/films in compliance with the European Commission's Decision on re-use of Commission's documents (2011/833/EU) for information or education purposes only. The personal data of registered members is not used for any automated decision-making including profiling.
8	**Description of the categories of data subjects**
	Whose personal data are being processed? ☐ 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: 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) Although informed via the data protection notice, Community members may voluntarily submit or share their image and voice during online events, in videoconferencing, audio calls, video recordings and/or podcasts (including shortened/edited versions and automated captions of these); (including as part of an application process for the accelerator programme[1]); and also including promotional videos for the European Digital Education Hub (such as anniversary videos and short videos with information about speakers at upcoming event). 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 pictures for articles to be published within the European Digital Education Hub or externally.

[1] For information about the accelerator programme, see Accelerator programme: unlocking innovation in digital education - European Education Area

	Promotional videos for the European Digital Education Hub (e.g., anniversary videos) may include voices of narrators. 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 European Digital Education Hub or externally. 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 in general or in specific sub-areas covered by the European Digital Education Hub After registration, Community members may provide information on their personal motivation to join the European Digital Education Hub's Higher Education Interoperability Workgroup (in a separate registration) ; 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) Where applicable, to allow for remuneration of experts' work, their bank details are 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 or optional, depending on the category) Mandatory: All Community members must share their current professional role and field of work when registering. Optional: Individuals who are interested in registering as an "expert" may 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). Mandatory: Individuals who are interested in joining the Workgroup/Expert Group on Higher Education Interoperability must 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, experience with the topic of interoperability or a project managed). Mandatory: In the context of calls for experts or calls for participation or contribution (including calls for "squad" participants), providing information on the career of the Community members, their experiences with the topic of the event/squad, their motivation/interest in the event/squad and their intended follow-up actions after the event/squad is mandatory as it serves as selection criteria. Mandatory: 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. Optional: In the context of preparation 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 EUSurvey questionnaires. Optional: In the context of articles to be published within the European Digital Education Hub or externally, Community members may voluntarily share their experiences, opinions and quotes/testimonials. Optional: In the context of interviews, selected interviewees may be asked to provide additional information on their latest experience of relevance of the topic of the interview as well as general information on their current institutional affiliation and professional role. Optional: Podcasts are recorded with active practitioners and experts, who can share their insights and views on digital education. These are recorded and disseminated to the wider Hub community. In the context of podcast, participants may record audio files with their

	voices, as well as information about their names, career background and institutional affiliation. These are collected through EUSurvey forms. ☐ 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 needs 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. The first name, last name, e-mail address and physical address of the narrators, whose voices are included in the European Digital Education Hub promotional videos (e.g., anniversary videos), are collected through authorisation forms (through EUSurvey) and kept on file. ☒ Other (optional) Community members may voluntarily share their food preferences (allergies, vegetarian options, halal, etc.) when registering for physical events where food is served. Community members may voluntarily share their special needs (such as accessible entrance to meeting rooms) when registering for physical events. To ask for assistance when facing technical problems with MS Teams, registered members may share screenshots providing information about their personal computers, internet connection and account settings, such as IP addresses and Microsoft account usernames. ☒ Other (mandatory) Community members attending physical events, such as community workshops and design-thinking workshops, must sign participants/attendance lists when arriving physically to the event. The signatures of mentors who sign mentorship agreements and squad leaders who sign squad contracts are also collected. ***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 *(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, application, or authorisation purposes is kept for four years from the respective event. Personal data collected through EUSurvey and processed for the accelerator programme application purposes is kept until 07.02.2025. 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 collected on **Newsroom** The retention periods of the personal data of users collected through the European Commission's corporate tool Newsroom are established in data protection record No. DPR-EC-03928. Personal data processed on the **Europass platform** The retention periods of the personal data of users collected through the Europass are established in data protection record No. DPR-EC-04686.2. Personal data in **promotional videos** The European Digital Education Hub promotional videos with personal data (e.g., voice, first name, last name, country of origin, professional role, testimonials) may be hosted and / or published on the Audiovisual Service of the European Commission, on other European Commission or EACEA websites and/or corporate platforms for four years from the start of the service contract between the data controller and the above-mentioned data processors (i.e., until 07.02.2026). Personal data may be used and archived by the European Commission in accordance with data protection record No. DPR-EC-00074.2. Personal data in **interviews and articles** Personal data in interviews and articles (e.g., photos, first names, last names, professional role, institutional affiliation, country of origin, experiences, opinions, and quotes/testimonials) is kept for up to 5 years from the date of consenting to the corresponding authorisation form. Personal data included in **written outputs** published by the Publications Office of the European Union Personal data included in written outputs published by the Publications Office will be stored for as long as the output is publicly accessible. Personal data in **social media posts**

	Personal data published on the EUDigitalEducation X (former Twitter), see account and the Erasmus+ Facebook page(s) of the European Commission (e.g., photos, first names, last names, professional role, institutional affiliation, country of origin and quotes/testimonials) is kept in accordance with the privacy policy of X (former Twitter) (see https://x.com/en/privacy) and Facebook (see https://www.facebook.com/privacy/policy). Personal data gathered for **physical events** Data gathered for physical events (except regarding travel to/from the events, mentioned below), and the personal data gathered via EUSurvey) is kept for 48 months from the respective event. Live-streaming, photos and audio-visual recordings of events is also kept for 48 months from the start of the service contract between the data controller and the above-mentioned data processors (i.e., until 07.02.2026), or 5 years from the event, if this is indicated in the application form and/or the event-specific DPN. . Personal data concerning **pay, allowances and bank accounts and missions and journeys**, as well as **signatures** on attendance/participants lists, are kept for 10 years after the service contracts in order to comply with the audit/accounting obligations of the responsible data processors. Personal data in email requests for **technical support** Personal data gathered in requests for technical support will be kept for four years from the start of the service contract between the data controller and the above-mentioned data processors (i.e., until 07.02.2026). Personal data in podcasts Personal data gathered in podcast recordings will be kept for four years from the start of the service contract between the data controller and the above-mentioned data processors (i.e., until 07.02.2026). **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), the Directorate-General for Informatics (DG DIGIT), the Directorate-General for Communications Networks, Content and Technology (DG CNECT), the Directorate-General for Communication (DG COMM) and the Directorate-General for Employment, Social Affairs and Inclusion (DG EMPL). • 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. • Recipients listed in data protection record No. DPR-EC-00074.2 with regard to videos published on the Audiovisual Service of the European Commission. • Recipients included in data protection record No. DPR-EC-04686.2 concerning the Europass “badges”. • Additional recipients mentioned in data protection record No. DPR-EC-03928 regarding the newsletter subscriptions on Newsroom. • Authorised staff of the processors identified in section 6, and the following sub-processors: 1) European Schoolnet Partnership AISBL, Belgium (see http://www.eun.org/legal-notices-and-privacy), 2) Learning Planet Institute (LPI), France,

	(see https://www.learningplanetinstitute.org/en/legal-notices/) 3) Knowledge Innovation Centre Ltd. (KIC), Malta (see https://knowledgeinnovation.eu/wp-content/uploads/2025/03/2024_privacy-policy_knowledgeinnovation.eu_.pdf), 4) Open Evidence SL, Spain (see https://open-evidence.com/privacy-policy/), 5) Deloitte Consulting GmbH, Germany (see https://www.deloitte.com/de/de/legal/privacy.html), 6) SURF U.A. Cooperative, Netherlands (see https://www.surf.nl/en/privacy-statement-surf-bv) . • Registered members of the Community who have access to personal data available or shared on a voluntary basis in the MS Teams channels. • Upon consent, personal data may be shared with the general public through publication and dissemination on the Internet, in particular on the European Education Area Portal, the Audiovisual Service of the European Commission, other European Commission or EACEA websites and/or corporate platforms, the Publications Office of the European Union, as well as on the EUDigitalEducation X (former Twitter) account and the Erasmus+ Facebook page(s) of the European Commission. The European Digital Education Hub newsletter may be archived by EACEA and the European Commission, including in the European Commission's Newsroom archive. It may also be hosted on the archived web page of the Publications Office of the European Union. • Registered members who have been selected to be part of community workshop Programme Committees and/or squad leaders will have access to the data mentioned above: "information on the career of the Community members, their experiences with the topic of the event/squad, their motivation/interest in the event/squad and their intended follow-up actions after the event/squad". The general public will also have access to any publication (including images) via the webside of EACEA and /or the EC , 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, in the context of TEAMS, your data may be transferred to the U.S. in certain circumstances as specified in the Privacy Statement for M365. This transfer is based on the Adequacy Decision adopted by the European Commission for the EU -U.S. Data Privacy Framework. SLIDO may be used in accordance with its privacy policy which can be found here: https://ec.europa.eu/dpo-register/detail/DPR-EC-06687 . Participants not willing to share their personal data with the selected tool can simply reply anonymously. As SLIDO was acquired by Cisco, personal data may be transferred to Cisco in the US and the U.K. based on the related Adequacy Decisions adopted by the European Commission. Moreover, upon consent, personal data may be published on Facebook and X (former Twitter) social media accounts of the European Commission, which can trigger a transfer of personal data outside the EU in accordance with the respective social media privacy policies (see Facebook (https://www.facebook.com/privacy/policy) and X (https://x.com/en/privacy) accordingly). Such transfers are based on the explicit consent of the data subjects under Article 50(1)(a) of Regulation (EU) 2018/1725. In such cases, the data subjects are informed that the level of protection of personal data will depend on the law and/or practice of the third country, which might offer a lower level of protection of the personal data compared to the EU legislation. Personal data with other third-party tools – including Miro boards – are not gathered; participants are explicitly asked to not enter any personal data in these. However, IP numbers may be gathered in these. See their respective privacy statement: • https://miro.com/trust/privacy-and-governance/ Miro is on the list of the EU-U.S. Data Privacy Framework for the Adequacy Decision adopted by the European Commission for the U.S.
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 No. 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. **Management of subscriptions on Newsroom**

	The technical and organisational security measures implemented to ensure information security are defined in section 8 of data protection record No. DPR-EC-00841 .4. **Europass platform** The technical and organisational security measures implemented to ensure information security are defined in section 8 of data protection record No. DPR-EC-04686.2. **Audiovisual Service of the European Commission** The technical and organisational security measures implemented to ensure information security are defined in section 8 of data protection record No. DPR-EC-00074.2. **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.

Learning Planet Institute (LPI)'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.

Knowledge Innovation Centre Ltd. (KIC)
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.

Open Evidence SL
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.

Deloitte Consulting GmbH
Deloitte has implemented and continues to maintain appropriate strong state-of-the-art technical, organisational and management measures to keep personal data secure and safe from loss, damage, corruption or deletion. Data is being stored in the Netherlands and Ireland,

	respectively on-premises in Germany. In case data is being accessed by sub-processors of Deloitte (Spanish-based Deloitte Consulting S.L.U. Spain), contracts are signed to ensure that sub-processors secure data according to GDPR. SURF U.A. Cooperative (SURF) To uphold the highest standards of data protection and integrity, SURF employs a robust and comprehensive data management strategy. Data at SURF is stored on advanced encrypted servers, both onsite and on selected cloud platforms in the EU, ensuring data sovereignty and compliance. Strict access protocols are in place, permitting only authorised personnel with a defined need-to-know basis to access any personal data. Regular audits are conducted to verify that all practices remain in line with SURF's information security policy and to promptly address any potential vulnerabilities.
14	**Information to data subjects / Privacy Statement**
	The data protection notice attached to the EUSurvey registration form is available on the General MS Teams channel of the Community under "Files" and also in the European Digital Education Hub instructions manual.