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 European 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 03-2022

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 Art 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.

European School Education Platform

1 Last update of this record (where applicable)

Last update on 24/04/2024.

2 Short description of the processing

The European School Education Platform (referred hereunder as the ‘Platform’ or as 'ESEP') is the successor of the School Education Gateway and the eTwinning platforms.

Launched in 2022, this multilingual online Platform aims to be the meeting point for all school staff (from early childhood education and care to primary and secondary levels, including initial vocational education and training), researchers, policy makers and other stakeholders in the school education field.

Personal data is provided in 2 layers:

1. Registration with EU login “ad general” users, to access and participate in the activities (such as online courses or submit listings) and to use all the available features of the Platform (commenting on articles, adding items in favourites, or saving searches).

2. Additional registration as eTwinning user (eTwinner).

At the launch of ESEP, the existing users of eTwinning and/or of the School Education Gateway must create an EU Login account with the same email address initially used when registering on eTwinning and/or School Education Gateway, in order to synchronise the old with the new account, including migration of personal data.

A specific area of the Platform is ‘eTwinning’. It offers a restricted area for school staff (ex. teachers, head teachers, librarians*)* in one of the countries associated, to collaborate, develop projects, share, and engage in the community. Users applying to the eTwinning area must be validated by the National Support Organisations (of their countries) to be granted access, to be able communicate, collaborate, meet, chat, develop projects, participate in professional development activities.

The Platform has a Professional Development Advisory Board (referred here as ‘’PDAB’’) that supports the strategic development of the Platform itself and the eTwinning activities linked to the professional development of teachers and other key actors. It is composed by 2 representatives from the National Support Organisations, 2 representatives from the eTwinning Ambassadors, and 2 representatives from the ESEP Supportive Partners. Personal data of PDAB members is processed for the purpose of preparing a memorandum of understanding summarising the terms of cooperation between European Schoolnet and PDAB members.

The National Support Organisations of eTwinning engage in online activities on the European Commission’s Microsoft 365 environment. Data processing is necessary to register the members of the National Support Organisations to give access to the Microsoft (MS) Teams platform, and to allow them to engage in the eTwinning Community activities conducted on the MS Teams platform.

Part 1 - Article 31 Record

3 Name of the Controller
Unit(s) and/or function of person acting on behalf of the Controller

	Controller: European Education and Culture Executive Agency (EACEA) Officer designated in charge of the processing operation: Head of Unit EACEA.A6: Platforms, Studies and Analysis Email: eacea-eplus-esep@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. EUN Partnership AISBL (hereinafter called European Schoolnet) runs the ESEP including eTwinning Central Support Service (CSS) as a contractor of EACEA. Rue de Trèves, 61 (3rd floor) 1040 Brussels, B Tel: +32 2/790 75 75 Email: info@eun.org Website: www.eun.org European Schoolnet's sub-processors are: • HOFI: Hofi studio SRO (printing and design studio) (Ruska 77, 100 00 Prague 10, CZ) – sylva@hofi.cz • UBIQUS BADGES France (access management) (10 Rue de la plaine, 78860 Saint Nom la Bretèche, FR) – lmerad@ubiqus.com • Connections-Eurotrain NV (travel services) (Luchthavenlaan 10, 1800 Vilvoorde, B) – b2b@connections.be • Eagle Travel (travel services) (Chausée de la Hulpe 192, 1170 Watermael-Boitsfort, B) – business@eagletravel.be Local audiovisual partners are occasionally hired to create on-site recordings on behalf of European Schoolnet, in countries where this capacity is not available locally. Their involvement is limited to the creation of recordings and transfer to European Schoolnet. Address and contact details vary, depending on the assignment, and can be made available upon request. 2. Tremend Software Consulting SRL provides the digital services needed to manage and maintain eTwinning.net, also as contractor of EACEA. 83 Cluj Stroot, bl. 8B, sc. 1, floor 7, ap.32 030134 Bucharest, RO Tel: +40-21-223-7700 Email: hello@tremend.com Website: https://tremend.com

The European Commission Directorate-General for Informatics (DG DIGIT) provides the IT hosting service for ESEP.

Some components of ESEP require interactions with the Commission's Microsoft Office 365-instance, with the Commission's EUSurvey platform, with the Commission's EU Academy e-learning platform, and with the Commission's EU Login platform, but these are autonomous services operated by the European Commission (as set out in Section 7 below) rather than sub-processors to European Schoolnet or Tremend.

7 Purpose of the processing

The purpose of processing personal data of registered users is to operate ESEP and provide related services such as:

- Allow the operation of the Platform's services such as:
  - posting comments and listings
  - accessing features such as favourites or save searches
  - enriching users' profiles
- Handle helpdesk inquiries, follow-up on posts and messages reported
- Allow communication and collaboration in the spirit of mutual trust and respect
- Facilitate the follow-up and monitoring activities of the community as well as the performance of ongoing research activities disseminated on the Platform
- Develop outreach and communication purposes within the framework of the Platform and its services,
- Send newsletters related to the Platform and to the eTwinning to inform on updates and relevant information within European Commission's initiatives
- Enable online trainings – both organisation and implementation
- Enable and improve the user experience within this (and similar future) project(s) developed by the European Commission via access control, tracking of usage frequency, search behaviours, preferences and settings
- Allow the collection, categorisation, and summary of user contributions in the fora and other discussion tools
- Provide aggregated statistics, including, but not limited to, the number of users during a specific period, the preferred subjects and/or countries chosen by users and account usage, to evaluate the access patterns and user preferences / requirements
- Provide users with certificates of completion of online trainings
- Produce and disseminate videos and podcasts featuring interviews with experts and best practices of schools and teachers
- Conduct various surveys regarding the Platform services and open calls for participation in focus groups of researching in various pedagogical fields
- Allow the publication of articles on the Platform
- Evaluate and support the security and correct operation of the Platform, and the lawfulness of its use.

Furthermore, and limited to eTwinning, the processing of personal data is necessary to:

- Provide information about registrants' activities within and outside the eTwinning area to establish and maintain online community's activities
- Allow registrants to find partners and set up projects
- Provide information about the eTwinning projects
- Allow eTwinning registrants to communicate and collaborate in the spirit of mutual trust and respect
- Allow and facilitate monitoring and research activities

- Produce and disseminate videos featuring best practices of schools, teachers, users of eTwinning, winners of the eTwinning European Prizes
- Provide users with certificates of completion of online courses, in digital and print, and / or trophies in relation to the eTwinning European Prizes, eTwinning School Labels, National and European Quality Labels
- Conduct surveys regarding the services of the Platform and for participants in the focus groups withing the various pedagogical issues
- Participate in webinars, online events, and onsite events.

For the coordination of the National Support Organisations of eTwinning (see Point 2) MS Teams is used (a third-party data processor). The framework of the MS collaborations is defined in the data protection record for the European Commission's Microsoft 365 environment (reference No. DPR-EC-04966). The personal data of registered members will not be used for any automated decision making, including profiling.

For the surveys as well as the focus group registrations carried out through the Platform and eTwinning area, EUSurvey is used. The full information about the processing of personal data under EUSurvey is defined under the record No. DPR-EC-01488.

Finally, and limited to participation in the courses taking place on the EU Academy, the processing of data – which will take place at the EU Academy – is necessary to:

- Enrol the user to the course selected, and
- allow the access the course in the EU Academy environment while keeping the credentials.

The names, emails, and course selection of ESEP users following training courses will be shared with and processed by the European Commission's EU Academy for the purposes of providing such trainings, following the EU Academy privacy policies (see record No. DPR-EC-05546.1). Data on the progress of learners and the outcome of the training course will be shared with the European School Education Platform for the purposes as set out above (including gathering and sharing training credentials).

8 Description of the categories of data subjects

Whose personal data are being processed?
☒ EACEA staff (Contractual and temporary staff in active service)
☐ 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: individuals registered on the European School Education Platform or in the eTwinning restricted area (validated school staff) and any person participating in the activities organised by the eTwinning users, recipients of the surveys conducted through the Platform and/or the eTwinning area, individuals registered for the events, focus groups, webinars, online courses promoted within the eTwinning area and/or the Platform, experts, teachers, users of eTwinning, interviewed winners of the eTwinning European Prizes, certificate holders, online / onsite events attendees, EU Academy course participants, newsletter subscribers, users who choose to share articles on the Platform, PDAB members. In addition, contact details of National Support Platform are published on the Platform.

9 Description of personal data categories

Indicate all the categories of personal data processed and specify which personal data are being processed for each category (between brackets under/next to each category):

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),
Optional personal information can be added to the user profile; a registrant can decide whether to give that data or not. The optional information entails images. Images and / or sound data of the participants who take part in the onsite events conducted in the scope of activities of the Platform and / or eTwinning may be collected.
Speakers and participants who take part in online events and/or podcasts may voluntarily submit or share their image and voice during the online events, in videoconferencing, audio calls, video recordings and / or podcasts. Image and / or sound data of the experts, teachers, users of eTwinning, winners of the eTwinning European Prizes who are interviewed and/or who share their best practices are collected.

☒ concerning the data subject's private sphere
Information from fora and other online communication tools: the Platform offers public fora (or similar third-party communication tools) as part of its collaborative spaces. On these online tools, users choose whether to share comments, thoughts, photos, videos and / or other information on a voluntary basis. The Platform also allows the choice to interact with third party tools; however, these tools apply their own privacy policies which are clearly shared with end-users and fall outside the scope of this Record.

□ concerning pay, allowances, and bank accounts

☒ concerning recruitment and contracts:
Personal data of the PDAB members.

□ concerning the data subject's family

☒ concerning the data subject's career
The Platform may receive personal identifiable information when data is provided in response to a survey (in such cases, users are requested prior consent to share the information). If the participant takes part in an online training or in a project, certain student-generated content may be collected, such as the assignments submitted, peer-graded assignments and peer grading student feedback. Course data is also gathered, such as student responses to quizzes, fora entries and surveys.
In the context of events preparation, confirmed participants may be asked to submit information on their intended follow-up actions post event through EUSurvey questionnaires.
In the context of articles to be published on the Platform, participants may voluntarily share experiences, opinions, pictures and quotes.

□ concerning leave and absences

☒ concerning missions and journeys
Participants may take part in events onsite in their own country or in another one. They may submit information for the purpose of participating in such initiatives. To be able to be reimbursed for the travel, the accommodation and for subsistence costs and events badges for onsite activities, information on itineraries and travel receipts need to be collected.

□ concerning social security and pensions

□ concerning expenses and medical benefits

□ concerning telephone numbers and communications

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

☒ Other: please specify:
For eTwinning users, the school and the professional role at the school is mandatory. The National Support Organisations representatives should upload themselves the personal data (contact details and name of the organisation).

Participants taking part in an onsite event may share dietary preferences (allergies, vegetarian options, halal, etc.) when registering to events where a meal is foreseen. The personal data on nutritional restrictions is used solely for the purposes of meals planning and the names are not shared with the catering vendor.

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 – data relating to food allergies)
□ genetic data, biometric data for the purpose of uniquely identifying a natural person
□ concerning sex life or sexual orientation.

It is possible that unsolicited personal data of this nature is submitted by the data subjects. This action is however not encouraged in any way, and any information of this nature will be disregarded and not substantively processed.

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)

A. For the **general users** registered on ESEP the data related to the profile is kept for three years after the user’s last login. After these three years, the user profile will automatically be set to anonymous, i.e. the personal data will be erased.

Two weeks prior to the deadline of these three years of no login, a notification is sent to the user to inform her/him that her/his profile is about to be set as anonymous and that he/she can avoid this by logging in again within two weeks. If the user does not login within two weeks, his/her profile will be deleted permanently. In case of no login, all personal information is then made anonymous.

Any personal data the user may have inserted through third parties’ tools (e.g. during an online course when using an external online tool, such as Facebook or X) may be stored and processed by that third party. Such processing does not fall within the scope of this Record and is therefore not affected by the anonymisation.

If users ask for the anonymisation of their account, or the account is automatically anonymised, no data will be visible to other ESEP users. If users with an anonymised account want to continue using the Platform, they will need to register again. The anonymised data (non-personal data) remains solely for research and monitoring purposes at the disposal of EACEA, the European Commission, national or regional school authorities, authorities in charge of implementing the ESEP and other third parties (see Point 6) under the authorisation of the data controller and in an aggregated format.

B. Regarding the data related to the profiles of **eTwinning users**, the personal data is kept for a maximum of three years after the user's last login. After one year from the last login, the user profile will automatically be set to inactive, i.e., no longer visible to other users nor the outside world. The user can re-activate her/his account by logging in again. A reminder is sent after two additional years informing the user that, three years after her/his last login, his/her profile will be anonymised.

If users request for the anonymisation of their account, or the account is automatically anonymised, the personal data will be erased.

Data will be kept only in an anonymous format that does not allow any personal identification. If users with a deleted profile want to continue using the Platform, they will need to register again. The data remain solely for research and monitoring purposes at the disposal of EACEA, the European Commission, national or regional school authorities, authorities in charge of implementing eTwinning (Central Support Service and National Support Organisations) and other third parties (see Point 6) under the authorisation of the Data Controller in an aggregated format.

C. Regarding certain data processing activities carried out in relation to the Platform and / or eTwinning area, specific data retention periods apply. Concretely:

- Personal data collected through the EUSurvey tool for registration to focus groups are kept for 2 years after the end the current service contract, including the periods of extension.

- Personal data collected in the context of newsletters' subscription, is kept during the period that users keep this option active, i.e., up to the withdrawal of consent to receive newsletters. In any case, data will not be kept longer than 2 years after the end the current service contract, including the periods of extension.

- Personal data collected for the purposes of producing videos, podcasts and photos of interviewees are only used in information / publicity materials produced for a maximum of 2 years after the end the current service contract, including the periods of extension.

- Personal data related to the organisation and management of the events or webinars (this includes the information given during the registration, prior, during or after the event or webinar) as well as live-streaming and audio-visual recordings of events or webinars, is kept for 3 years after the event or webinar concerned for the purpose of sharing further information with the participants on future related events or webinars. Personal data regarding dietary requirements of the participants in onsite events are deleted promptly at the conclusion of the event concerned.

- Personal data collected on the Commission's MS Teams, the Identification data is stored for as long as the member's account is active. Service generated data (log files) are kept for up to 6 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 5 years upon expiration / termination of the subscription.

- Personal data of the PDAB members is retained for 10 years upon expiration / termination of the subscription to fulfil the contractual obligations.

- Personal data entrusted to Ubiqus Badges as part of the management of their service will be stored for a maximum period of 10 years upon expiration / termination of the badges.

- Personal data concerning missions and journeys will be kept for 10 years after such mission / journey 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.

11 Recipients of the data

For the purposes detailed above, access to the full set of data is strictly limited to:

- EACEA designated staff
- European Commission designated staff, in particular DG EAC and DG DIGIT and, for personal data of users following training courses on the EU Academy platform, and JRC designated staff
- Authorised staff of the organisation contracted and working on behalf of EACEA to implement ESEP, i.e. Central Support Service (European Schoolnet) and digital service provider (Tremend Software Consulting SRL).
- Recipients identified in data protection record ￼￼No. DPR-EC-01488￼ concerning the processing made via EUSurvey (Privacy Statement under Point 7)
- Other sub-processors of European Schoolnet as listed under Point 6.
- In rare cases if IT issues are not solved by the EC DG DIGIT Microsoft Teams and other recipients identified in data protection record No. DPR-EC04966 concerning processing made via Microsoft Teams (Privacy Statement under Point 7)
- General Public: Some data submitted by users will be displayed on the public area of the Platform and on social media, meaning that such information is freely accessible on the Internet. In this case, users have the possibility to delete their data.

The data which may be, upon the user's decision, made public, is the following:

a) **Organisation data of the user** is visible to all users through the organisation's page and on related third parties (social media)

- name, address, city, country, picture, Facebook URL, X URL, LinkedIn URL and website
- registrants affiliated to the organisation (first name, last name, country, picture)
- courses, and Erasmus+ postings created by members of the organisation.

b) **ESEP (General) user data**:

- the following user data is visible to all users only on the public organisation's page (if the user is affiliated to one or several organisations): first name, last name, country, a thumbnail of the picture (if provided)
- user's profile page is accessible only to other logged-in users, including the following information: first name, last name, country, picture, organisation(s), user type, comments made by the registrant, articles 'favourited' by the user, and whether the registrant is eTwinning validated
- any postings and comments voluntarily made by a registered user is public, i.e. visible to the website users and retrievable through search engines
- user's activities on the online trainings are viewable only by the registered users to that specific online training.

The transfer of specific data to other third parties (e.g., research centres and universities) can be permitted under specific authorisation of the data controller, but data will be transferred in an aggregated and anonymous format.

Some personal data will be accessible within the restricted area of eTwinning, eTwinning Groups and TwinSpaces only to the respective members of these areas.

Some data based on consent may also be posted on social media (acting as separate controller).

c) eTwinning users' data

Access to the eTwinners data is strictly limited to:

- eTwinning validated users (upon login) can see the following data of other users: full set of data except users' email address and school leader's data
- authorised staff of EACEA and the European Commission (such as DG EAC and DG DIGIT): full set of data
- Authorised staff of the organisation contracted by EACEA to implement the eTwinning component of ESEP, i.e. Central Support Service (European Schoolnet) and digital service provider (Tremend Software Consulting SRL): full set of data
- National Support Organisations: have access to registration data submitted on eTwinning.net to be able to validate / manage their registration and certain activities (National Support Organisations have only access to the data of users of their respective countries)
- JRC designated staff for personal data of eTwinners who decide on a voluntary basis to follow training courses on the EU Academy 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 or authority 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 of 12 June 2019 laying down general implementing provisions on the conduct of administrative inquiries and disciplinary proceedings – C(2019)4231 and Commission Decision (EU) 2019/165 of 1 February 2019 on the internal rules concerning the provision of information to data subjects and the restriction of certain of their data protections 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
- The European Data Protection Supervisor.

Personal data is never shared with third parties for marketing purposes (other than the Platform's own newsletter as mentioned above).

12 Are there any transfers of personal data to third countries or international organisations? If so, to which ones and with which safeguards?

Aventri – Stova Group, LLC

Concerning eTwinning, there are transfers of personal data into third countries, as some National Support Organisations are based outside the European Union (EU) or the European Economic Area (EEA) in the following countries: Albania, Algeria, Armenia, Azerbaijan, Bosnia and Herzegovina, Georgia, Jordan, Lebanon, Moldova, Montenegro, North Macedonia, Serbia, Tunisia and Türkiye. The transfers to these countries are necessary for important reasons of public interest and are based on Article 50(1)(d) of Regulation (EU) 2018/1725 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 European Union

The Erasmus+ Programme funding this process encourages the participation of young people in Europe's democratic life, including by supporting activities that contribute to citizenship education and participation projects for young people to engage and learn to participate in civic society, thereby raising awareness of European common values (see Recital n° 28 of the Erasmus Regulation (Regulation (EU) 2021/817)).

The National Support Organisations are equally bound by data protection clauses, particularly in relation to lawfulness of processing and technical and organisational security obligations, under a grant agreement signed with EACEA.

The transfer occurring concerns the validation of the users by their respective National Support Organisations and in the case the user applies for prizes and quality labels. Therefore, the transfer is limited to this verification process. National Support Organisations only receive personal data of users of their own base-country. The users may request a copy of these clauses by contacting the controller. The data processor is bound by data protection clauses under a service contract signed with EACEA.

Other data submitted by users on the eTwinning component of the Platform (e.g., messages in fora, online discussions and threads, files and pictures) are only visible amongst registered users within the area of the Portal where they have been uploaded (e.g., eTwinning Groups, TwinSpace). Some of these users may be based in third countries.

In very few cases, limited personal data from MS Teams may be transferred to the United States, as foreseen in section 6 of data protection record No. DPR-EC-04966. Such transfers are subject to appropriate safeguards, namely the adequacy decision with the United States since its entry into force in 2023.

13 General description of the technical and organisational security measures

DATA CONTROLLER

The European Commission's IT systems used by EACEA abide by the Commission's security guidelines. EACEA 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.

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

Organisational measures include appropriate access rights and access control. As a rule within EACEA, 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 EACEA staff are bound by a confidentiality obligation. The need-to-know principle applies in all cases.

2. 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.

The Platform servers are hosted on Amazon Web Services in the 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.

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 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.

A contractual clause about data protection is included in the contract with the processors (service providers) EUN Partnership AISBL and Tremend Software Consulting, to ensure that personal data are processed in compliance with the applicable legislation.

3. Additional measures at the level of processors and sub-processors

i. Processor

European Schoolnet has put in place appropriate technical and security measures to protect the premises, systems, applications, and databases where personal data is stored against accidental lost, alteration, disclosure or use or access in an unauthorised way.

European Schoolnet processes only the personal data required for achieving the purposes communicated to the data subjects prior to such collection and restricts access to personal data to European Schoolnet designated staff and specified third party sub-processors with a business need to know. The specified sub-processors process personal data only on behalf of the European Schoolnet. The European Schoolnet only discloses the strictly necessary personal to sub-processors to provide their services and does not allow the use personal data for their own purposes. Pursuant to the special clause added to the agreements concluded with the sub-processors, they are bound to process personal data in accordance with the GDPR and to implement appropriate procedures to prevent loss, damage, or interference with such data as well as to keep the data secure.

All data collected by the European Schoolnet is stored on secure servers based in the EU. Access to the servers is strictly limited to European Schoolnet designated staff. European Schoolnet has included in data processing terms with the specified third-party sub-processors to ensure that personal data processed on behalf of European Schoolnet by such sub-processors is stored on the sub-processors' EU-based servers and is not transferred outside the EU without prior authorization.

The Technical Team has put in place an Acceptable Use Policy applying to all its staff (employees, contractors, in-house consultants, temporary staff) governing the use of the technical infrastructure and office equipment. 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 DPO. Any data breach is reported without delay to EACEA and the Technical Team comprised by members of EUN. Tremend supports EACEA in collecting the facts before making an informed decision under the EUDPR (notification to the EDPS, communication to the data subjects). The circumstances surrounding the breach are also investigated to prevent future breaches.

ii. Sub-processors

HOFI is required by EACEA to process data in compliance with the requirements of the EUDPR and shall not engage another processor without the specific written authorisation of EACEA.

Aventri/Stova has implemented appropriate technical, organizational, and administrative measures to protect personal data from unauthorized access, disclosure, misuse, alteration, or loss. These measures include security controls to prevent unauthorized access to their facilities and systems, strong authentication procedures and strict password protection protocols, utilizing encryption software for all financial and other sensitive personal data transmitted on or through their sites, and conducting regular penetration tests. Aventri/Stova affirms that it complies with additional data processing requirements for personal data originating in the EU, as required by the GDPR and has contractual obligations to host data in the EU.

Ubiqus Badges guarantees that it implements all the technical, legal and operational measures necessary to ensure the confidentiality of this data and will ensure that all persons authorized to process it, whether internal or external to the group, comply with this obligation. Ubiqus Badges will inform the data controller within 24 hours in the event of a data breach. Furthermore, Ubiqus Badges commits to take reasonable steps to destroy or anonymize personal data when no longer needed and also to protect personal data against unauthorized access, disclosure, loss, misuse, and alteration.

14 Information to data subjects / Privacy Statement

ESEP Privacy Statements for general users and for eTwinning users are available here.

For other tools that the Platform interacts with (EU Login, the Office 365 instance, EUSurvey etc), separate policies are provided as indicated in their respective records.