EUROPEAN EDUCATION AND CULTURE
EXECUTIVE AGENCY (EACEA)

Development of the European Higher Education Sector Observatory (EHESO)

Data Protection Notice

The European Education and Culture Executive Agency ("EACEA") is committed to preserving the protection of your personal data. This notice provides information on your rights in relation to data protection and on how your personal data are processed by EACEA in accordance with Regulation (EU) No 2018/1725 on the protection of personal data by the Union institutions, bodies, offices and agencies[1] ("the Data Protection Regulation").

1. Who is responsible for processing your personal data (data controller)?

The controller is EACEA , BE-1049 Brussels
The person designated as being in charge of the processing operation is the Head of Unit A.6 Platforms, Studies and Analysis
The contact email address is EACEA-HE-OBSERVATORY@ec.europa.eu

2. For which purpose do we process your data?

Your personal data are collected and used to develop a functional European Higher Education Sector Observatory, which must be able to collect the most relevant data, allow the informed people to use this data for their own analysis, engage relevant persons into various working groups and events contributing to the development of EHESO, and inform various public and specialised audiences about the EHESO results. These includes:

- Organise an event (which include registrations, sending the agenda, sharing link(s) to evaluation, etc.);
- Take pictures / video and record the event;
- Send newsletters, surveys,

This is because EACEA is mandated by the European Commission to implement the ERASMUS+ Programme.

Your personal data will not be used for an automated decision-making including profiling.

3. Which personal data are processed?

In order to carry out the processing operation, the following data may be processed:

- Names, surnames;

[1] 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 Text with EEA relevance, OJ L 295, 21.11.2018, p. 39.

- function;
- contact details (email address, business telephone/GSM numbers, postal address, company and department, country of residence, internet address);
- Bank account reference (IBAN and BIC codes), VAT number, passport number, ID number;
- Diet and/ or accessibility requirements and related consent
- photos, videos and meeting recordings and related consent

The provision of personal data is mandatory to meet a contractual requirements of service contract SI2.905534 as per Call for Tenders Call for tenders EACEA/2023/OP/0004 . If you do not provide your personal data, possible consequences are the exclusion from the activity.

4. Who has access to your personal data and to whom is it disclosed?

Access to your personal data is provided to the EACEA staff responsible for carrying out this processing operation and to any authorised staff according to the "need to know" principle. Such staff abide by statutory confidentiality obligations.

The following recipients may also access to your personal data :

- Authorised staff of the European Commission such as DG EAC, CNECT, DIGIT, etc

- Authorised staff of the EACEA contractor(s) acting as processor(s) : PPMI Group[2], Austrian Institute of Technology GMBH (AIT)[3], Gemeinnutziges Centrum Fur Hochschulentwicklung GMBH (CHE)[4], Joanneum Research Forschungsgesellschaft MBH[5], Universiteit Twente[6] that abide by contractual confidentiality requirements. For more information on how your data may be processed by them, please have a look at their privacy statements. Please note that only the data mentioned in this data protection and in line with the conditions stipulated herewith are processed by the contactor(s).

- Public access for data published on https://eter-project.com/ or https://national-policies.eacea.ec.europa.eu/ websites and/or on the social media of DG EAC (X, Facebook, etc)

The following third-party tools and services are used: e.g. Facebook, with their applicable privacy statement[7].

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.

The information we collect will not be given to any third party, except to the extent and for the purpose we may be required to do so by law.

In addition, data may be disclosed to public authorities in accordance with Union and Member State law such as the European Court of Justice, the relevant national judge as well as the lawyers and the agents of the parties in case of legal proceedings, the Investigation and Disciplinary Office of the European Commission (IDOC), the competent Appointing Authority in case of a request or a

[2] https://ppmi.lt/who-we-are#:~:text=At%20PPMI%2C%20we%20are%20committed,EU)%202016%2F679).
[3] https://www.ait.ac.at/en/disclaimer-data-protection
[4] https://www.che.de/en/privacy/
[5] https://www.joanneum.at/en/datenschutz/
[6] https://www.utwente.nl/en/cyber-safety/privacy/gdpr/
[7] https://www.facebook.com/privacy/policy/

complaint lodged under Articles 90 of the Staff Regulations, the European Anti-Fraud Office (OLAF), the Internal Audit Service of the Commission (IAS), the Court of Auditors, the European Ombudsman, the European Data Protection Supervisor (EDPS) and the European Public Prosecutor's Office (EPPO).

5. How long do we keep your personal data?

EACEA only keeps your personal data for the time necessary to fulfil the above-mentioned purpose and follows the Common Retention List of the European Commission.(CRL).

- Personal data (first name, last name, job position, organisation, country of residence, e-mail address) of persons, who will provide data and information about their (higher education) institutions and countries, will be kept for 4 years after collecting such data. It is notable that the initial EHESO contract is for 2 years, but can be extended for 4 years. Therefore, 4 years are set as a period of storage for such data. In case the contract is not extended, the personal data mentioned in this point will be deleted 2 years after collecting it.
- Personal data (first name, last name, job position, organisation, country of residence, e-mail address, signature, possibly also voice and image, food preferences and special needs) of persons, who will attend EHESO online and physical events and working groups, will be kept for 4 years after the registration to the relevant event or a working group. It is notable that the initial EHESO contract is for 2 years, but can be extended for 4 years. Therefore, 4 years are set as a period of storage for such data. In case the contract is not extended, the personal data mentioned in this point will be deleted 2 years after collecting it.
- Personal data (first name, last name, job position, organisation, country of residence, e-mail address) of persons, who will register to receive the EHESO Newsletter, will be kept for 5 years after registering to the Newsletter. According to the Newsroom wiki: "Personal data is kept for a period of 5 years after the last interaction with the Commission services or until the user request the deletion of his/her personal data. It refers to 5 years after the last interaction of the data subject with Newsroom. For subscribers it counts from the last subscription date or last change in his/her subscription. It is important to note that receiving a newsletter or a notification item is not considered an "interaction" for this purpose. "Interactions" are actions from the subscriber with the Newsroom application such as subscribing, confirming a subscription, updating a subscription, updating his/her profile (name, surname, etc.). "
- Personal data (first name, last name, job position, organisation, country of residence, e-mail address) of persons, who will register to access EHESO microdata will be kept for 4 years after the registration. It is notable that the initial EHESO contract is for 2 years, but can be extended for 4 years. Therefore, 4 years are set as a period of storage for such data. In case the contract is not extended, the personal data mentioned in this point will be deleted 2 years after collecting it.
- 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.
- After expiration of the contract, personal data may be kept for financial verification/audit purposes and for a period of 5 years from the last payment linked to this contract.

6. How do we protect and safeguard your personal data?

Relevant organisational and technical measures are taken by EACEA to ensure the security of your personal data.

Technical measures include appropriate actions to address online security, risk of data loss, alteration of data or unauthorised access, taking into consideration the risk presented by the processing and the nature of the personal data being processed.

Organisational measures include restricting access to the personal data solely to authorised persons with a legitimate need to know for the purposes of this processing operation. Access to your data is done via authentication system on an individual basis through user-ID and password. Your data resides on the servers of the European Commission, which abide by strict security measures implemented by the European Commission (DG DIGIT) to protect the security and integrity of the relevant electronic assets. EACEA is also bound by Commission Decision 2017/46 of 10/1/17 on the security of communications & information systems in the EC.

EACEA's contractors are bound by a specific contractual clause for any processing operations of your data on behalf of the Commission, and by the confidentiality obligations deriving from the transposition of the General Data Protection Regulation in the EU Member States ('GDPR' Regulation (EU) 2016/679.

The European Commission's IT systems used by the Agency 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.

Organisational measures by EACEA:

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 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.

Technical measures by EACEA:

State of the art technical cybersecurity measures are implemented in the corporate systems, according to the security needs. Those measures are in constant evolution.

Organisational and technical measures in relation to data collection from statistical and national authorities (ETER data collection):

The only personal data collected in the process of ETER data collection will be the contact details (emails, first names, last names and phone numbers) of contact persons at national statistical authorities. This personal data will be collected from the websites of the national statistical authorities and included in an Excel document, which will be placed in a secure server of the EHESO consortium (Joaneum Nextcloud). This personal contact data will be accessible only to the selected authorised staff with a login and a password. This personal data will be used exclusively to contact the relevant staff of the national statistical authorities in order to ask for the relevant data.

Organisational and technical measures in relation to authorisation to use EHESO microdata:

Organisational measures include a strict separation of access to the server itself and the applications running on the server. This means that only a very limited number of people may access the server. The number of people who have administrator rights in the application is also very limited. Access is granted on the principle of least privilege.

Technical measures include the implementation of a wide range of cybersecurity measures, such as hardening the servers according to the CIS benchmark. Each part of the application is only executed with the rights that are absolutely necessary for execution and is additionally hardened where possible (e.g. the web server, where system hardening further reduces privileges). Additional scans of the applications are used to minimise the risk of supply chain attacks.

OrgReg authentication is controlled by RISIS – Research Infrastructure for Science and Innovation Policy Studies, who will act as a data sub-processor in this case.

Organisational and technical measures in relation to survey of institutions and students:

For both institutional and student surveys, personal data of institutional coordinators are used to manage the surveys. The personal contact data of institutional coordinators is gathered from the websites of higher education institutions.
Personal data of coordinators include:

- Name, first name.
- Gender.
- E-mail address.
- Unit and function.
- Institutional affiliation.

Data are stored in a php/MySQL data base, running on a protected CHE server accessible only to the authorized staff through the login and the password.
Personal data of the coordinators are used to inform institutions about the course and process of the institutional and student survey.
As the participating institutions are sending invitations to their students to participate in the student survey, we will not have any personal student data.

Organisational and technical measures in relation to collaboration of working groups in the Commission's MS Teams environment:

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. The access to the MS Teams channels of the Community is limited to "owners" and "guests". Only specific teammates have access to private channels.

Organisational and technical measures in relation to various events organised in the context of EHESO:

For online events, the European Commission's MS Teams environment will be used. The 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. The access to the MS Teams channels of the Community is limited to "owners" and "guests". Only specific teammates have access to private channels.

Physical events will be organized by limited dedicated teams of staff working at EHESO consortium partners. Only these staff members will have access to personal details of the participants (such as first name, last name and e-mail address, food preferences or special needs related to accessibility). All lists of participants will be stored in secure servers.

Organisational and technical measures in relation to EHESO Newsletter:

The newsletter uses the European Commission (EC) corporate tool (Newsroom) managed by DG CNECT, which abide to the European Commission's security directives and provisions established by the Directorate of Security for these kinds of servers and services.
Contractors

Organisational and technical measures in relation to EHESO contractors:

EACEA's contractors have contractual obligations to adopt technical and organisational security measures to process personal data processed in the framework of this contract.

7. What are your rights concerning your personal data and how can you exercise them?

Under the provisions of the data protection regulation, you have the right to request to the controller to access the personal data that EACEA holds about you and to have your personal data rectified in case your personal data are inaccurate or incomplete.
Where applicable, you have the right to request the erasure of your personal data and to restrict the processing of your personal data.
You are also entitled to object to the processing of your personal data on grounds relating to your particular situation at any time unless EACEA demonstrates compelling and overriding legitimate grounds or in case of legal claims.

When processing is based on your consent, you have the right to withdraw your consent at any time, without affecting the lawfulness of the processing before such a withdrawal.

However, the data controller may restrict the rights of the data subjects based on article 25 of the Data Protection Regulation (in exceptional circumstances and with the safeguards laid down in the Regulation. Such restrictions are provided for in the internal rules adopted by EACEA and published in the Official Journal of the European Union.[8]

Such a restriction will be proportionate, limited in time, and respect the essence of the above-mentioned rights. It will be lifted as soon as the circumstances justifying the restriction are no longer applicable. In principle, you will be informed on the principal reasons for a restriction unless this information may cancel the effect of the restriction. A more specific data protection notice may apply in such case.

8. Contact Information

If you have questions or wish to exercise your rights under the Data Protection Regulation or if you want or to submit a complaint regarding the processing of your personal data, you are invited to contact the Data Controller (see contact details above).

You can also contact the Data Protection Officer of EACEA at the following email address: eacea-data-protection@ec.europa.eu.

You may lodge a complaint with the European Data Protection Supervisor: http://www.edps.europa.eu.

[8] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32021Q0317%2801%29

9. On which legal basis are we processing your personal data?

We process your personal data, because:

- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body (as laid down in Union Law);
- the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

- Council Regulation 58/2003 of 19 December 2002, laying down the Statute for executive agencies to be entrusted with certain tasks in the management of EU programmes ;
- Commission Implementing Decision (EU) 2021/173 of 12 February 2021 establishing the European Education and Culture Executive Agency;
- Commission Decision C(2021)951 of 12 February 2021 delegating powers to the European Education and Culture Executive Agency with a view to the performance of tasks linked to the implementation of Union programmes in the field of education, audiovisual and culture, citizenship and solidarity;
- Regulation (EU) 2021/817 establishing the Erasmus+ programme

The following special category(ies) of personal data is (are) being processed: health data (diet requirement).

We process special categories of personal data indicated above, because the data subject has given explicit consent to the processing for one or more specified purposes.