EUROPEAN EDUCATION AND CULTURE
EXECUTIVE AGENCY (EACEA)

RECORD OF PERSONAL DATA PROCESSING

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

Record nº *2024- 08*

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.*

Development of the European Higher Education Sector Observatory (EHESO)	
1	**Last update of this record (where applicable)**
	Not applicable
2	**Short description of the processing**
	EHESO aims to leverage the strengths of existing EU data tools and capacities, including the European Tertiary Education Register (ETER), U-Multirank, Erasmus+ database, Database of External Quality Assurance Results (DEQAR), Eurostudent, Eurograduate, Eurydice higher education data from the Bologna Process Implementation Reports, Mobility Scoreboard, and other relevant data sources. Additionally, the integration of new tools to further enhance their

	utility and relevance within the context of the strategy is to be explored. This holistic approach will yield a wealth of indicators, benchmarks, analyses, and reports specifically designed to satisfy the requirements of policymakers, European higher education institutions, students, academics, and researchers alike. EHESO is operated by a consortium of organisations, under a service contract with the European Education and Culture Executive Agency (EACEA). The consortium implementing the European Higher Education Sector Observatory is coordinated by PPMI Group, UAB. The following organisations are involved as partners of the consortium: Centre for Higher Education (CHE), Center for Higher Education Policy Studies (CHEPS) at the University of Twente, AIT Austrian Institute of Technology and Joanneum Research. The following are activities of EHESO which will require processing of personal data: • Data collection from statistical and national authorities (ETER data collection). • Authorisation to use EHESO microdata. • Survey of institutions. • Survey of students. • Working groups. • Various events organised in the context of EHESO. • EHESO Newsletter. Personal data processing will be necessary to achieve three main goals of EHESO: • To collect the necessary data from various subjects: national and statistical authorities, higher education institutions, students. • To engage the necessary persons in EHESO working groups and events. • To inform the general and specialised publics about the EHESO results and events. • To allow authorised persons to use EHESO microdata for their research purposes. For processing personal data, EHESO consortium will prioritises the European Commission's Microsoft 365 environment (e.g. the European Commission's MS Teams for events and working groups) and other EU corporate tools such as EACEA's Newsletter tool and EUSurvey tool.
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 Unit(s): Head of Unit A.6 Platforms, Studies and Analysis EACEA-HE-OBSERVATORY@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. PPMI Group, UAB (as consortium leader) Legal form: Private Company - Joint Stock Company Statutory registration number: 300654654 Address of registration: Gedimino pr. 50 LT-01110 Vilnius Data protection contact point: personaldata@ppmi.lt As consortium members: 2. AIT AUSTRIAN INSTITUTE OF TECHNOLOGY GMBH Legal form: Private Company - Gesellschaft mit beschränkter Haftung (GmbH) Statutory registration number: FN115980 i Address of registration: GIEFINGGASSE 4 1210 WIEN – AT Data protection contact point: office@ait.ac.at 3. CHE GEMEINNUTZIGES CENTRUM FUR HOCHSCHULENTWICKLUNG GMBH Legal form: Non-profit limited company Statutory registration number: HRB 3122 Address of registration: VERLER STRASSE 6 33332 GUTERSLOH – DE Data protection contact point: datenschutz@che.de 4. JOANNEUM RESEARCH FORSCHUNGSGESELLSCHAFT MBH Legal form: Private Company - Gesellschaft mit beschränkter Haftung (GmbH) Statutory registration number: FN 48282 d Landesgericht für Zivilrechtssachen Graz Address of registration: LEONHARDSTRASSE 59 8010 GRAZ – AT Data protection contact point: datenschutzbeauftragter@joanneum.at 5. UNIVERSITEIT TWENTE Legal form: Public Law Body - Universtity Statutory registration number: 50130536 Address of registration: DRIENERLOLAAN 5 7522 NB ENSCHEDE – NL Data protection contact point: fg@utwente.nl DG DIGIT/ European Commission for the use of M365 services in line with the agreement MICROSOFT ILA (DI/07880) signed with EACEA DG CONNECT for the use of Newsroom
7	**Purpose of the processing**
	The overall purpose of personal data processing is to develop a functional European Higher Education Sector Observatory, which could fulfil the expectations raised for it in the European Strategy for Universities. Functional EHESO 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. The following will be the specific purposes of processing personal data: • To collect the necessary data from various subjects: national and statistical authorities, higher education institutions, students. In this case, contact details (such as name, surname, job position and email address) of persons is used to gather the relevant data from these persons. The data provided by these persons will not be personal data, and will describe characteristics of their institutions or country-level higher education sectors.

<table>
<tr><td></td><td>

To engage the necessary persons in EHESO working groups and events (both online and on site). In this case, contact details (such as name, surname, job position and email address) of persons is used to invite them to the online and physical events or online collaboration tools (such as MS Teams channels). Engaging in events and working groups also means that these persons, if they chose so, may share their voice or image with the EHESO consortium staff (e.g. by participating with audio and video in online calls or coming to a physical event). Persons coming to the physical events are asked to sign attendance lists.
To inform the general and specialised publics about the EHESO results and events. In this case, contact details (such as name, surname, job position and email address) of persons is used to send them a newsletter about EHESO events and results.
To allow authorised persons to use EHESO microdata for their research purposes. In this case, contact details (such as name, surname and email address) of persons is used by them to apply for EHESO's authorisation, so that they can access EHESO microdata.
To engage members in the Community activities on the MS Teams platform and allow them to communicate, network and collaborate through posts, reactions and chats.
To allow for the analysis of members' feedback on Community activities (the main objective being quality monitoring and improvement).
Upon consent, to inform about European Higher Education Sector Observatory results and developments, upcoming events and/or other related initiatives of the European Commission through a dedicated newsletter.

Individuals interested in participating in activities (such as surveys) 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).
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). The personal data of registered members will not be used for any automated decision-making including profiling.
</td></tr>
<tr><td>8</td><td>Description of the categories of data subjects</td></tr>
<tr><td></td><td>
Whose personal data are being processed?
In case data categories differ between different categories of persons, please explain as well (e.g. suspects vs. witnesses in administrative inquiries)
☒ Agency staff (Contractual and temporary staff in active position)
☐ Visitors to the Agency
☒☐ Applicants
☐ Relatives of the data subject
☐ Complainants, correspondents and enquirers
☐ Witnesses
☐ Beneficiaries
☐ External experts
☒ Contractors
☒ Other, please specify: persons providing data about institutions and countries (such as staff of national and statistical authorities, staff of higher education institutions), persons participating in EHESO events, persons participating in EHESO working groups, persons authorised to use EHESO microdata, persons subscribed to EHESO Newsletter.
</td></tr>
</table>

9	**Description of personal data categories**
	Indicate <u>all</u> 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 or voice (Data subjects may voluntarily submit or share their image and voice during online or physical events, in videoconferencing, audio calls and/or video recordings. They may decide to voluntarily share their picture(s) in public or private channels of the MS Teams platform. When it comes to physical events, the registration forms for the physical event will explicitly ask if the participants agree to be pictured or recorded.) ☐ concerning the data subject's private sphere ☒ concerning pay, allowances and bank accounts ☐ concerning recruitment and contracts ☐ concerning the data subject's family ☒ concerning the data subject's career (In some cases, the data processors may ask for the current job position of the data subject and the name of the organisation that he/she represents as well as information on education .) ☐ concerning leave and absences ☒ concerning missions and journeys ☐ concerning social security and pensions ☐ concerning expenses and medical benefits ☒ concerning telephone numbers and communications (In some cases, to ensure the ease of communication the data processors may ask for the telephone numbers of data subjects.) ☒ concerning names and addresses (including email addresses) (In most cases, the data subjects will be asked to provide their first names, last names, and e-mail addresses. In some cases, the data subjects may also be asked to provide their country of residence.) ☒ Other: please specify: Data subjects may share their food preferences (allergies, vegetarian options, halal, etc.) on a voluntary basis when registering for physical events where food is served. Data subjects may share their special needs (such as accessible entrance to meeting rooms) when registering for physical events. Data subjects may share their signature when signing the list of participants in physical events.) ***b) Categories of personal data processing likely to present <u>specific risks:</u>*** ☐ data relating to suspected offences, offences, criminal convictions or security measures ☐ data being used to evaluate personal aspects of the data subject (ability, efficiency, conduct) ***c) Categories of personal data whose processing is <u>prohibited</u>, with exceptions (art. 10):***

	☐ revealing racial or ethnic origin ☐ revealing political opinions ☐ revealing religious or philosophical beliefs ☐ revealing trade-union membership ☒ concerning health ☐ genetic data, biometric data for the purpose of uniquely identifying a natural person ☐ concerning sex life or sexual orientation ***d) Specify any additional data or explanatory information on the data being processed, if any:*** N/A
10	**Retention time (time limit for keeping the personal data)**
	Indicate the period of storage: • 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.

	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**
	• Authorised staff of EACEA and the European Commission, in particular the Directorate-General for Education, Youth, Sport and Culture (DG EAC), Directorate-General for Communications Networks, Content and Technology (CONNECT) and the Directorate-General for Informatics (DG DIGIT). • Authorised staff of the processors identified in section 6. • Microsoft Teams and other recipients identified in data protection record No. DPR-EC-04966 concerning processing made via Microsoft Teams. • Recipients identified in data protection record No. DPR-EC-01488 concerning processing made via EUSurvey. • Persons who have access to personal data available or shared on a voluntary basis in the MS Teams channels (e.g. participants in the working groups revealing their name, surname or email to other working group participants). • 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[1]. In addition, in case of control or proceedings personal data can be shared with and processed by the bodies charged with a monitoring, judicial or inspection task in application of Union law in compliance with the applicable data protection rules and within the scope of their tasks entrusted by the relevant legislation. This includes, in particular, the following recipients: • 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 European Anti-Fraud Office (OLAF); • The Internal Audit Service of the Commission • The Investigation and Disciplinary Office of the Commission (IDOC) • The European Court of Auditors • The European Ombudsman • The European Public Prosecutor's Office • The European Data Protection Supervisor (EDPS) • National authorities
12	**Are there any transfers of personal data to third countries or international organisations? If so, to which ones and with which safeguards?**
	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
13	**General description of the technical and organisational security measures**
	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. 1. Organisational measures by EACEA:

[1] https://www.facebook.com/privacy/policy/

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.

2. 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.

3. 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.

4. 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.

5. 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. 6. 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. 7. 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. 8. 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. 9. 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.
14	**Information to data subjects / Data Protection Notice (DPN)**
	The information on the specific operations related to processing personal data will always be sent or made available to the data subjects in the form of specific Data Protection Notice.