



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 n°

01-2022

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.

Erasmus+ National Focal Points (ENFPs)	
1	Last update of this record (where applicable) 23/05/2022 (initial version)
2	Short description of the processing EACEA collects and processes personal data in order to establish a global network of Erasmus+ National Focal Points (ENFPs). The purpose of the network is to create a support structure that will be an essential component in the implementation of the Erasmus+ programme (2021-2027). The ENFPs will provide information and on-the-ground advice to potential applicants and beneficiaries. They will have a key role in supporting the Erasmus+ programme's objectives and impact by ensuring that it becomes known and readily accessible to all potential applicants, irrespective of the sector. ENFPs personal data are also collected and processed by the service contractor offering a Centralised Support to the Network of ENFPs (SPENFP) for the purpose of organising the activities foreseen in the tender, including via registration on a Virtual community website.

	<p>Given the essential role the ENFPs have in the Erasmus+ Programme providing information and on-the-ground-advice, the contact information of the ENFPs will be made public on the Virtual community website to ensure that all interested potential applicants can contact them. It is planned to have a contact form on the website through which the individual ENFPs can be reached which will be developed and managed by the SPENFP service provider.</p> <p>The ENFP contact details will also be used for networking within that group and for meetings with, the EACEA, other Commission services, National Agencies, the National Erasmus+ Offices, local Erasmus+ stakeholders. It is foreseen that the ENFPs and the above mentioned institutions will meet at networking events online and in person.</p> <p>Considering the variety of events and activities to be organised under the SPENFP service contract, <u>additional processing might be carried out and further explained in the applicable data protection notice.</u></p>
Part 1 - Article 31 Record	
3	<p>Name of the Controller Unit(s) and/or function of person acting on behalf of the Controller</p> <p>Controller: European Education, and Culture Executive Agency Head of Unit A4 Erasmus+: Higher Education – International Capacity Building EACEA-EPLUS-ENFP@ec.europa.eu</p>
4	<p>Contact details of the Data Protection Officer (DPO)</p> <p>EACEA-data-protection@ec.europa.eu</p>
5	<p>Name and contact details of joint controller (where applicable)</p> <p>N/A</p>
6	<p>Name and contact details of processor (where applicable)</p> <p>The following service provider runs the SPENFP platform on behalf of EUROPEAN EDUCATION AND CULTURE EXECUTIVE AGENCY (EACEA):</p> <p>PRACSIS PIC 972441782 Legal form: Private company Address of registration: PLACE COMMUNALE D'AUDERGHEM 8 1160 BRUXELLES Country of registration: BE</p>
7	<p>Purpose of the processing</p> <p>Nomination of ENFPs:</p> <p>The information is collected in order to be able to contact the ENFPs and to establish a network so the ENFPs can communicate with each other.</p> <p>The ENFPs will be nominated by the competent authorities in each country, often the national Ministry of Education. This information is communicated to the EU Delegation in the country. The latter informs the EACEA about the nomination. EACEA is responsible for storing the contact information and updating the information when necessary. It is EACEA's purpose to keep the contact details of the ENFPs in order to be able to contact the network and to be able to establish and animate a network within the ENFPs.</p>

	<p>ENFP activities:</p> <p>ENFPs personal data are also collected and processed by the service contractor offering a Centralised Support to the Network of ENFPs (SPENFP).</p> <p>EACEA will communicate the ENFPs contact details to the service contractor for the purpose of involving them in the activities (online and in situ) foreseen in the tender. For the same purpose ENFP contact details will be published.</p> <p>In addition, ENFPs, as well as other participants, will register on the Erasmus Networks Platform (https://erasmus-networks.ec.europa.eu/landing-page/au-homepage) for events, trainings, networking and other activities organised by the service provider. For training purposes, ENFPs will also register to EU Academy (EU Academy (europa.eu)).</p> <p>The platform provides a mechanism of information, communication and coordination, to ensure a smooth functioning of the ENFP network. The web platform serves as a communication tool for the ENFP community, as a source of information and as a registration website for events. The personal data is collected so that the Agency and its service provider can have regular contacts with the members of the ENFP network for training and information purposes. Making the personal data visible to registered users also facilitates networking between individual ENFPs. The personal data collected is needed:</p> <ol style="list-style-type: none"> To invite ENFPs to register as users of the Erasmus Networks Platform, grant them access to the European Commission's MS Teams platform or Webex for specific events organised by EACEA 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, take part in mentoring activities, take part in workshops, seminars, conferences), which may also be part of a process of selecting candidates for activities with limited numbers of participants To engage members in the Community activities on the platform and allow them to communicate, network and collaborate through posts, reactions and chats To organise and manage online events (e.g. workshops, web-seminars, stakeholder meetings and round tables, online meetings, trainings, mentoring activities, peer-learning) through audio-visual conferencing and/or recording To offer and manage other online learning activities (e.g., e-learning modules, webinars, etc.) To organise and manage physical events, including to contact the participants regarding organisational information (e.g., agenda, travel expenses, hotel, organising networking dinners and lunches in compliance with food allergies declared by participants); and to illustrate, promote or document the physical activities To document conducted activities and showcase the best digital solutions by submitting digital artifacts (e.g., minutes, publications, reports, news items, case studies and/or other outputs) To allow for the analysis of members' feedback on Community activities (the main objective being quality monitoring and improvement) 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 To inform about results and developments, upcoming events and/or other related initiatives of the European Commission through a dedicated newsletter To handle helpdesk inquiries and to provide technical support To be able to provide inclusive and accessible settings at physical events. <p>ENFPs will also register in MS Teams (Dedicated ENFP and SPENFP channels, as well as participation in online meetings) for information and communication purposes. 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 personal data of registered members will not be used for any automated decision-making</p>
--	---

	including profiling.
8	<p>Description of the categories of data subjects</p> <p>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)</p> <p><input type="checkbox"/> Agency staff (Contractual and temporary staff in active position)</p> <p><input type="checkbox"/> Visitors to the Agency</p> <p><input type="checkbox"/> Contractors providing goods or services</p> <p><input type="checkbox"/> Applicants</p> <p><input type="checkbox"/> Relatives of the data subject</p> <p><input type="checkbox"/> Complainants, correspondents and enquirers</p> <p><input type="checkbox"/> Witnesses</p> <p><input type="checkbox"/> Beneficiaries</p> <p><input checked="" type="checkbox"/> External experts</p> <p><input type="checkbox"/> Contractors</p> <p><input checked="" type="checkbox"/> Other, please specify:</p> <ul style="list-style-type: none"> - individuals nominated as ENFP by competent national authorities (often Ministries of Education) from non-EU countries. These people are not employed or paid by EACEA. - the designated staff of the EACEA, other EU Institutions (e.g. DG EAC, EU Delegations, DG INTPA, etc.), NEOs, National Authorities (e.g. Ministries) and other experts and users of the platform https://erasmusnetworks.ec.europa.eu/landing-page/au-homepage set up and managed by the service provider.
9	<p>Description of personal data categories</p> <p>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):</p> <p>a) Categories of personal data:</p> <p><input checked="" type="checkbox"/> in the form of personal identification numbers</p> <p><input checked="" type="checkbox"/> concerning the physical characteristics of persons as well as the image, voice or fingerprints</p> <p><input type="checkbox"/> concerning the data subject's private sphere</p> <p><input checked="" type="checkbox"/> concerning pay, allowances and bank accounts</p> <p><input type="checkbox"/> concerning recruitment and contracts</p> <p><input type="checkbox"/> concerning the data subject's family</p> <p><input checked="" type="checkbox"/> concerning the data subject's career (position and name of employer)</p>

	<p> <input type="checkbox"/> concerning leave and absences <input checked="" type="checkbox"/> concerning missions and journeys <input type="checkbox"/> concerning social security and pensions <input type="checkbox"/> concerning expenses and medical benefits <input checked="" type="checkbox"/> concerning telephone numbers and communications (telephone numbers and email addresses) <input checked="" type="checkbox"/> concerning names and addresses (including email addresses) (names and email addresses) <input checked="" type="checkbox"/> Other: please specify: title, academic title/position, gender, institution type, institution name, institution location, present position, qualification, field of expertise in higher education reform topics, academic field. Furthermore, whilst using the discussion forum function of the platform/MS Teams, data subjects can also submit any other personal data voluntarily. </p> <p>b) Categories of personal data processing likely to present <u>specific risks</u>:</p> <p> <input type="checkbox"/> data relating to suspected offences, offences, criminal convictions or security measures <input type="checkbox"/> data being used to evaluate personal aspects of the data subject (ability, efficiency, conduct) </p> <p>c) Categories of personal data whose processing is <u>prohibited</u>, with exceptions (art. 10):</p> <p> <input type="checkbox"/> revealing racial or ethnic origin <input type="checkbox"/> revealing political opinions <input type="checkbox"/> revealing religious or philosophical beliefs <input type="checkbox"/> revealing trade-union membership <input checked="" type="checkbox"/> concerning health <input type="checkbox"/> genetic data, biometric data for the purpose of uniquely identifying a natural person <input type="checkbox"/> concerning sex life or sexual orientation </p> <p>d) Specify any additional data or explanatory information on the data being processed, if any: _____</p>
10	<p>Retention time (time limit for keeping the personal data)</p> <p>The EACEA stores on the restricted O/U-Drive personal data of nominated ENFPs until the end of the Erasmus+ Programme in 2027, or until the end of their nomination if they are replaced before the end of the Programme.</p> <p>The personal data of ENFP is kept on the platform and the dedicated Microsoft TEAMS channel for the duration of their nomination.</p> <p>The personal data of the users of the Erasmus networks platform https://erasmusnetworks.ec.europa.eu/landing-page/au-homepage is kept up to three years following the last login. In case users request the deactivation of their profile or the profile is automatically deactivated, no data will be visible to other users. The data will be deleted and if users with a deactivated profile want to continue using the platform, they will need to register again.</p> <p>Personal data collected on MS Teams is processed and stored in line with the applicable</p>

	<p>data protection record No. DPR-EC-04966.4 https://ec.europa.eu/dpo-register/detail/DPR-EC-04966.4</p> <p>Personal data collected and processed via Webex is processed and stored in line with the applicable data protection record DPR-EC-05006.3 https://ec.europa.eu/dpo-register/detail/DPR-EC-05006.3</p> <p>Personal data collected and processed via EU Academy is processed and stored in line with the applicable data protection https://academy.europa.eu/admin/tool/policy/view.php?policyid=2.</p> <p>Is any further processing for historical, statistical or scientific purposes envisaged? <input type="checkbox"/> yes <input checked="" type="checkbox"/> no</p>
11	<p>Recipients of the data</p> <p>Personal data will be made accessible on need to know basis to the authorised staff within the following recipients:</p> <ul style="list-style-type: none"> - EACEA, - SPENFP service provider, - European Commission services, in particular DG EAC, INTPA, NEAR, - EU Delegations in third countries, - European External Action Service, - Erasmus+ National Agencies, - Erasmus+ National Offices (NEOs), - SPHERE service provider - EUSurvey (https://ec.europa.eu/eusurvey/home/privacystatement) - Erasmus Community platforms (https://erasmus-networks.ec.europa.eu/DPN) - General public: photos, video and audio recording including participants' personal data (face, presenters' contribution) may be published on the event webpage, as well as on the websites and intranet of EACEA and the European Commission and social media (and their corresponding privacy statement apply), namely Twitter, LinkedIn and Facebook. Publication of video and audio recording can be via a third party tool such as Vimeo. - Members of the MS TEAMS channel where the recording will be published, namely the Erasmus+ National Focal Points (ENFPs), EACEA, EC and the EU Delegations etc. <p>Furthermore, email address and name of the ENFPs will be accessible to the entire ENFPs network and published on the internet.</p> <p>Contractors/third party tools used with the corresponding privacy policy that applies. Participants not willing to share their personal data with the following contractors/tools are recommended to use them by inserting their organisation's name or other anonymous data:</p> <p>Contractors:</p> <ul style="list-style-type: none"> - Microsoft Teams (https://ec.europa.eu/dpo-register/detail/DPR-EC-04966 - see point 7 for the privacy statement) - Webex (https://ec.europa.eu/dpo-register/detail/DPR-EC-05006 - see point 7 for the privacy statement), - SLIDO: https://ec.europa.eu/dpo-register/detail/DPR-EC-06687 (see point 7 for privacy statement) <p>3rd party tools:</p> <ul style="list-style-type: none"> - Zoom (https://explore.zoom.us/en/trust/privacy/), - Padlet /'Wallwisher' (https://legal.padlet.com/privacy), - Caspio (https://www.caspio.com/caspio-privacy-statement/) - EventBrite (https://www.eventbrite.fr/help/fr/articles/460838/politique-de-confidentialite-d-eventbrite/)

	<ul style="list-style-type: none"> - MailChimp /'Intuit' (https://www.intuit.com/privacy/statement/) - Vimeo (https://vimeo.com/privacy) - Gutenberg Certs (https://www.gutenbergcerts.com/terms-of-service), - Mentimeter (https://www.mentimeter.com/trust/legal/privacy-policy) - Kahoot (https://trust.kahoot.com/privacy-policy/), - Hopin (https://support.streamyard.com/hc/en-us/articles/15401585037204-Privacy-Policy) <p>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:</p> <ul style="list-style-type: none"> - 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 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 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 of the EC Treaty 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	<p>Are there any transfers of personal data to third countries or international organisations? If so, to which ones and with which safeguards?</p> <p>For the organisation of certain events taking place in third countries, the booking of travels and accommodations of participants can be made either by the participants directly or by the contractor, which will require the collect and transfer of personal data into these third countries. Such booking and subsequent transfers of personal data will be made upon the explicit consent of the data subjects (Art 50.1(a)).</p> <p>For these countries, the EU has not adopted an adequacy decision pursuant to Article 47 of Regulation (EU) 2018/1725, hence certifying that the personal data once transferred, will benefit from an adequate level of protection in the third country of destination. Therefore, the transfer of data to those country applicable will be based either on standard contractual clauses and supplementary measures or on explicit consent.</p> <p>For the 3rd party tools mentioned under recipients above, the adequacy decisions of the European Commission for the US and for Canada applies for most of them (eg: companies appear in the US-EU Data protection framework certification list – see below).</p> <p>The following contractors / third party tools are covered by the adequacy decision of the European Commission for the US (EU data protection framework) and appear in the certification list.</p> <ul style="list-style-type: none"> - Microsoft Teams (https://ec.europa.eu/dpo-register/detail/DPR-EC-04966) - see

	<p>point 7 for the privacy statement)</p> <ul style="list-style-type: none"> - Webex (https://ec.europa.eu/dpo-register/detail/DPR-EC-05006 - see point 7 for the privacy statement), - Zoom (https://explore.zoom.us/en/trust/privacy/), - Padlet (https://legal.padlet.com/privacy), - Caspio (https://www.caspio.com/caspio-privacy-statement/), - EventBrite (https://www.eventbrite.fr/help/fr/articles/460838/politique-de-confidentialite-d-eventbrite/), - MailChimp (https://www.intuit.com/privacy/statement/) - Vimeo (https://vimeo.com/privacy). <p>The following third-party tool is covered by the adequacy decision of the European Commission for Canada.</p> <ul style="list-style-type: none"> - Gutenberg Certs (https://www.gutenbergcerts.com/terms-of-service), <p>In the privacy statement of the following third-party tools, they refer to the use of standard contractual clauses and appropriate safeguards ("appropriate agreements", "preventive measures", etc) to limit international transfers.</p> <p>Data subjects should be aware that some of the tools may transfer personal data to countries outside the EU/EEA which may offer a lower level of protection. They are therefore recommended to provide generic/non-personal data when using them (for instance, by registering with a corporate email address and the name of the organisation they work for instead of their personal data and/or email address).</p> <ul style="list-style-type: none"> - Mentimeter (https://www.mentimeter.com/trust/legal/privacy-policy) - Kahoot (https://trust.kahoot.com/privacy-policy/) - Hopin (https://support.streamyard.com/hc/en-us/articles/15401585037204-Privacy-Policy)
13	<p>General description of the technical and organisational security measures</p> <p>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.</p> <p>1. 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 DIGIT.</p> <p>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.</p> <p>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.</p> <p>The access to the EACEA building is protected and only persons with the right to enter are allowed.</p>

	The SPENFP service contract is managed by Pracsis, which is obliged by national law to apply a series of technical and organisations measures to ensure the protection of personal data. A data protection officer is responsible for ensuring that personal data are processed properly and kept secure in accordance with applicable regulations.
14	Information to data subjects / Privacy Statement <p>Data subjects will be informed about the processing of their data. This is done through the DPN at the first communication with the ENFP, when collecting their consent to share data with others. Data protection notice will also be made available on the platform, the relevant MS TEAMS channel, and as appropriate as part of the organisation of the activities.</p>