Ref. Ares(2022)3861573 - 23/05/2022

EUROPEAN COMMISSION
European Education, and Culture Executive Agency

RECORD OF PERSONAL DATA PROCESSING

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

Record nº *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)**
	N/A
2	**Short description of the processing**
	We will process 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. The contact information of ENFPs will not be made public but used only for networking within that group and for meetings with the EACEA, other Commission services, National Agencies and the National Erasmus+ Offices. It is foreseen that the ENFPs and

	the above mentioned institutions will meet at networking events online and in person. Furthermore, ENFP contact details will not be shared on the Erasmus+ website. 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 exclusively by DG EAC.
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): A4 EACEA-EPLUS-ENFP@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)**
	N/A
7	**Purpose of the processing**
	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. Moreover, the ENFPs can be contacted by National Erasmus+ Offices and other EU institutions for networking and communication purposes, programme implementation and monitoring purposes. 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.
8	**Description of the categories of data subjects**
	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) joining the TEAMS group ☐ 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 nominated by competent national authorities (often Ministries of Education) from non-EU countries. These people are not employed or paid by EACEA.
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, voice or fingerprints ☐ 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 (position and name of employer) ☐ concerning leave and absences ☐ concerning missions and journeys ☐ concerning social security and pensions ☐ concerning expenses and medical benefits ☒ concerning telephone numbers and communications (telephone numbers and email addresses) ☒ concerning names and addresses (including email addresses) (names and email addresses) ☐ Other: please specify: _____ ***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:*** _____
10	**Retention time (time limit for keeping the personal data)**
	Indicate the period of storage: EACEA will keep the data in the restricted O-Drive and in Microsoft TEAMS until either the ENFP wants to delete the information, until the national authority will change the contact person, or until the ENFP network ceases to exist. The data needs to be stored for this duration because the EACEA needs to have means to be able to reach out to the ENFPs and to ensure that they can network with each other. **Is any further processing for historical, statistical or scientific purposes envisaged?** ☐ yes ☒ no **If yes, indicate the further retention time:** If the answer is yes, please go to Part 2, Storage and Security for technical safeguards.
11	**Recipients of the data**
	Personal data will be made accessible on need to know basis to the authorised staff within the following recipients: - EACEA, - 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) Furthermore, email address and name of the ENFPs will be accessible to the entire ENFPs network. Third party tool used: Microsoft Teams. In addition, data may be disclosed to public authorities, and processed by these authorities in compliance with the applicable data protection rules according to the purpose of the processing, including inter alia: - The European Court of Justice or a national judge as well as the lawyers and the agents of the parties in case of a legal procedure; - The competent Appointing Authority in case of a request or a complaint lodged under Articles 90 of the Staff Regulations; - OLAF in case of an investigation conducted in application of Regulation (EC) No 1073/1999; - The Internal Audit Service of the Commission within the scope of the tasks entrusted by article 118 of the Financial Regulation and by article 49 of the Regulation (EC) No 1653/2004; - IDOC in line with Commission Decision 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	**Are there any transfers of personal data to third countries or international organisations? If so, to which ones and with which safeguards?**
	Transfers of personal data into third countries: personal data (name, surname, email address) of the ENFPs will be transferred outside the EU to the following recipients: other ENFPs who are based in different third countries of the world and who wish to join the network, including EEA and non-EEA Erasmus national agencies (North Macedonia, Serbia, Iceland, Liechtenstein, Norway, Turkey) and NEOs (Albania, Algeria, Armenia, Azerbaijan, Bosnia and Herzegovina, Egypt, Georgia, Israel, Jordan, Kazakhstan, Kosovo, Kyrgystan, Lebanon, Libya, Moldova, Morocco, Montenegro, Palestine, Russian Federation, Syria, Tajikistan, Tunisia, Turkmenistan, Ukraine, Uzbekistan). Please note that for these countries, the EU has not adopted an adequacy decision pursuant to Article 47 of Regulation (EU) 2018/1725, hence certifying that your personal data once transferred, will benefit from an adequate level of protection in the third country of destination. Therefore, the level of protection of your personal data transferred will depend on the law or practice of that third country and, as a result, your rights as regards data protection might not be equivalent to those in and EU/EEA country or a country with an adequacy decision. However, the NEOs are bound by data protection clauses, in particular with technical and organisational security obligations, under a grant agreement signed with the Agency. The users may request to obtain a copy of these clauses by contacting the controller. The NAs are bound by a contribution agreement with the European Commission, containing data protection clauses. However, ENFPs members will be able to give their explicit consent to the transfer of their personal data to these recipients, in accordance with Article 50(1)(a). Furthermore, please note that in order to deliver the service, Microsoft Teams might transfer your personal data outside the EU in accordance with its privacy policy. Such transfer will be made based on standard contractual clauses as part of a contract between the service provider and the European Commission. You can obtain more information on it by contacting the data controller at the above mentioned email address.
13	**General description of the technical and organisational security measures**
	1. Organisational measures: 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. For confidential files, access to documents is also limited based on a need to know rule. The access to the EACEA building is protected and only persons with the right to enter are allowed. All computers are password-secured. Access to the functional mailbox used for this purpose is given to a restricted number of staff on a need-to-know basis and all staff are bound by confidentiality obligations and other related legal obligations. 2. Technical measures: Technical measures include the use of secure equipment. The Agency's IT systems 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. The Agency's Corporate Local Informatics Security Officer (C-LISO) has the role of ensuring the Agency is compliant with this decision, and the application of security measures recommend by DIGIT.
14	**Information to data subjects / Privacy Statement** Data subjects will be informed about the processing of their data. This is done though the DPN at the first communication with the ENFP, when collecting their consent to share data with others. If ENFPs do not wish to share their personal data, they will have the choice of joining anonymously (for instance, by providing an anonymous address and a generic email such as Erasmus Focal point + country). When external beneficiaries wish to contact the ENFPs, a contact form on the Erasmus+ website will be created to get in touch with ENFPs. A separate DPN will be attached to it to inform those data subjects about how their personal data will be processed. This contact form will be set up and managed exclusively by EAC.

Electronically signed on 05/05/2022 10:57 (UTC+02) in accordance with Article 11 of Commission Decision (EU) 2021/2121