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 *2023-07*

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.*

Service contract for the Erasmus Mundus Support Structure (EMSS)	
1	**Last update of this record (where applicable)**
	N/A
2	**Short description of the processing**
	EACEA together with the EMSS Consortium (see below), service provider of EACEA, collects and processes personal data to allow the provision of services as defined in the Erasmus Mundus Support Structure tender specifications.

	The personal data is collected so that the Consortium can carry out the following activities: - Organise several events, presential and online (in the EU and also outside the EU); - Produce documentation (state of play reports, a study, different deliverables (representation structure needs analysis, scenarios, recommendations), for which input is required in the form of interviews, a survey and workshops (mostly online). - Manage an online community (Community of Practice).
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 Head of Unit A3 | Erasmus+, EU Solidarity Corps: Erasmus Mundus, Sport EACEA-A3-EM-SUPPORT-STRUCTURE@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 EMSS Consortium runs the EMSS contract on behalf of the European Education and Culture Executive Agency (EACEA): NTT DATA Belgique Official legal form: SRL Statutory registration number: 0712941486 Full official address: Rue de Spa 8, BE-1000 Bruxelles VAT registration number: BE0712941486 appointed as the leader of the group by the members of the group that submitted the joint tender TIPIK COMMUNICATION AGENCY SA Official legal form: S.A. Statutory registration number: 0435.539.007 Full official address: Avenue de Tervueren 270, BE-1150 Bruxelles VAT registration number: BE0435539007 ASSOCIATION POUR LA COOPERATION ACADEMIQUE - ACADEMIC COOPERATION ASSOCIATION Official legal form: Non-profit organisation (aisbl) Statutory registration number: 4022 94 Full official address: Rue d'Egmont 15, BE-1000 Bruxelles VAT registration number: BE0451407415 DEUTSCHER AKADEMISCHER AUSTAUSCHDIENST EV Official legal form: Registered Association (eingetragener Verein) Statutory registration number: VR 2107 Full official address: Kennedyallee 50, DE-53175 Bonn VAT registration number: DE122276332

	Sub-contractor : NTT DATA Spain SLU Official legal form: SLU Statutory registration number: Tomo 14.487, Hoja: M-239649, Folio 40, Sección 8, Inscripción 1ª Full official address: Camino Fuente de la Mora, 1, 28050, Madrid, Spain VAT registration number: B-82387770
7	**Purpose of the processing** The general objective of the Erasmus Mundus Support Structure is to provide Erasmus Mundus consortia with an environment for bottom-up exchange and networking, from the academic, pedagogical, scientific, and administrative points of view. To achieve this objective, several networking/awareness raising/information events are organised throughout the contract. The purpose of the data processing for events management is to be able to register participants for these events and ensure that their needs are catered for at the event. The contract also includes the production of a study and a series of state of play reports, which require input from stakeholders via different means: workshops, surveys, and interviews. List of activities throughout the contract that entail the processing of personal data as per tender specifications: - Organisation of 3 Large Scale Conferences: these events will gather up to 250 participants. - Organisation of 4 regional hybrid seminars (3 of them outside of the EU: Tokyo, Johannesburg (tbc) and Tbilisi (tbc): these events will gather up to 60 participants (in average, 30 presential, 30 online). - Organisation of 4 EMJM hybrid kick off meetings: these events will gather up to 60 participants (30 presential, 30 online). - Organisation of 4 worldwide webinars (info days): these events will gather up to 500 participants online. - Erasmus Mundus Anniversary Conference: this event will gather up to 400 participants. - Study on the impact of Erasmus Mundus: the study will be published. In order to gather data for the study, the following activities will be carried out: survey (no personal data collected), and expert workshops. - Publication of 7 State of Play Reports in the Community of Practice platform: These reports include input gathered through interviews. - Publication of 2 Study Visit Reports: These reports include input gathered through interviews. Next to the reports and studies that are going to be made public, the contract foresees a series of deliverables requiring input from experts, in the form of interviews, surveys, written contributions or calls for expression of interest. For organisational purposes, data on contributors might be collected in internal working files stored in the servers of the Consortium partners (i.e. name, surname and email).. Interviews might be recorded upon consent of the data subject only for internal use (minutes taking, preparing publications). Photos and recording may occur during all the above-mentioned activities and may be published on the Community of Practice (https://erasmus-networks.ec.europa.eu/erasmus-mundus, under construction, thus URL subject to change) and the Agency / EC websites (https://www.eacea.ec.europa.eu/index_en) for communication purposes.

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) ☐ Visitors to the Agency ☐ Contractors providing goods or services ☒ Potential applicants : Representatives of institutions interested to apply to the Erasmus Mundus calls for proposals and who will thus participate in the worldwide webinars (infodays) ☐ Relatives of the data subject ☐ Complainants, correspondents and enquirers ☐ Witnesses ☒ Beneficiaries who already receive funding from Erasmus Mundus ☒ External experts (interviewees for studies, speakers at events) ☒ Contractors ☒ Other, please specify: event participants, focus group participants
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 (NID / Passport numbers to organise travel for invited speakers / event participants) ☒ concerning the physical characteristics of persons as well as the image and voice as part of event recordings ☐ concerning the data subject's private sphere ☒ concerning pay, allowances and bank accounts (bank account to reimburse travel and accommodation costs) ☐ concerning recruitment and contracts ☐ concerning the data subject's family ☐ concerning the data subject's career ☐ concerning leave and absences ☒ concerning missions and journeys (travel arrangements for conference speakers and participants) ☐ concerning social security and pensions ☐ concerning expenses and medical benefits ☒ concerning telephone numbers and communications ☒ concerning names and addresses (including email addresses)

	☒ Other: please specify: data submitted voluntarily during interviews/activities, on MS TEAMS and/or on the platform, by answering questions during interview or tick box agreeing data to be used in a publication etc ***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*:* accessibility requirements for physical events; dietary requirements including food allergies for events catering. ☐ 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:*** NA
10	**Retention time (time limit for keeping the personal data)** **Period of storage**: Maximum of 132 months / 11 years (48 months / 4 years duration of the contract + 60 months / 5 years up to notification of audit + 24 months / 2 years to cover audit period). Personal data will be only processed for a limited period and erased thereafter. Considering the contract duration, the processing period will be of 48 months. After that period personal data will be blocked and only kept for the purposes of providing evidence to eventual project audits or exercising legal claims, in line with the provisions of the service contract, which states that the contracting authority can notify the contractor of an audit up to five years after the end of the contract. An additional two years (24 months) have been added to cover the provision of evidence for such an audit should it be required. Data concerning health (dietary restrictions) and disabilities collected for events is deleted one month after the event for which it was collected. The recordings of the interviews and of the events is kept for the duration of the contract (48 months / 4 years). The personal data of the users of the Erasmus Mundus Community of Practice https://erasmus-networks.ec.europa.eu/erasmus-mundus (under construction, thus URL subject to change) managed through Open Social is kept up to three years following the last login within the maximum duration of the contract (48 months). 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.

	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) and the Directorate-General for Informatics (DG DIGIT).
- Authorised staff of EMSS Consortium (data processors) as detailed in point 6 of part 1.
- Registered members of the Community of Practice who have access to personal data available or shared on a voluntary basis in the Community of Practice channels.
- General public when events/outputs (recording, pictures, surveys, etc) are made public on EACEA/EC websites
- Third party tools and other recipients identified in data protection records related to these tools:
  - Personal data collected during events organised with the technical support of DG Interpretation of the European Commission (SCIC) is processed and stored in line with the applicable data protection records No. DPR-EC-00306.1 https://ec.europa.eu/dpo-register/detail/DPR-EC-00306.1 and No. DPR-EC-00297.5 https://ec.europa.eu/dpo-register/detail/DPR-EC-00297
  - Personal data collected on EU Survey is processed and stored in line with the applicable data protection record No. DPR-EC-01488 https://ec.europa.eu/eusurvey/home/privacystatement
  - Personal data collected on Slido is processed and stored in line with the applicable data protection record No. DPR-EC-06687.1 https://ec.europa.eu/dpo-register/detail/DPR-EC-06687
  - Personal data collected on MS Teams is processed and stored in line with the applicable data protection record No. DPR-EC-04966.4 https://ec.europa.eu/dpo-register/detail/DPR-EC-04966.4
  - 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 (privacy statement: https://ec.europa.eu/info/files/web-conference-privacy-statement_en)
  - Personal data collected and processed via Doodle is processed and stored in line with Doodle's privacy policy: https://doodle.com/en/privacy-policy/

Personal data made public by registered Community members in the Community of Practice channels can be seen by other users. Some of them could be based outside the EU or the European Economic Area. The general public will also have access to any workshop content/outputs (including images) published by EACEA and/or the European Commission via the Internet, including on the Community of Practice.

In addition, in case of control or dispute, personal data can be shared with and processed by the bodies charged with a monitoring 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 - EU courts and 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 order to deliver online/hybrid events, Webex and/or Microsoft TEAMS may be used which might transfer personal data outside the EU in accordance with their privacy policy (see links to the respective records under point 11 above (recipients)). Such transfer will be made based on standard contractual clauses as part of a contract between the service provider and the European Commission. Limited personal data from MS Teams might be transferred to the United States as foreseen in section 6 of data protection record No. DPR-EC-04966.4 https://ec.europa.eu/dpo-register/detail/DPR-EC-04966.4, and from Webex to the United States and the United Kingdom as foreseen in section 6 of the data protection record DPREC- 05006.3 https://ec.europa.eu/dpo-register/detail/DPR-EC-05006.3. For the organisation of certain events taking place on site in countries outside the EU-EEA area or in third countries other than those covered by an adequacy decision, the registration of participants as well as the booking of travels and accommodations of participants can be made either by the participants directly or by the contractor, which will require the collection and transfer of personal data into these third countries. Such registration or booking and subsequent transfers of personal data will be made upon the explicit consent of the data subjects (Art 50.1(a)). 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 level of protection of the personal data transferred will depend on the law or practice of that third country and, as a result, the rights as regards data protection might not be equivalent to those in and EU/EEA country or a country with an adequacy decision.
13	**General description of the technical and organisational security measures**
	EACEA 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. 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.

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

NTT DATA

NTT Data has a Data Protection Office (DPO), responsible for defining, managing and supervising that NTT DATA complies with privacy regulations. It also provides training on personal data processing. The DPO is supported by its local representatives, usually represented by the Corporate Information Security Officers (CISO) to:

- ensure that the globally defined security and privacy measures are implemented;
- create a security culture by defining, developing and managing a local training and awareness programme;
- provide support to identify privacy and security risks in business proposals through expert advice;
- offer advice and monitor data protection breaches; and
- provide support and advice about approval processes and client audits in terms of data protection and security.

Organisational measures include appropriate access rights and access control to documentation

DAAD

DAAD has a Commissioner for data protection, responsible for defining, managing and supervising that DAAD staff complies with the privacy regulations. Data is stored on servers accessible to DAAD staff only, via a personal password.

DAAD's "Data Privacy Statement" can be found on the website (https://www.daad.de/en/data-privacy-statement/), comprising the following sections:

1. Data Processor and Data Protection Officer – contact details
2. Object of data protection
3. Type, scope, purposes and legal basis for data processing
3.1 Provision of our website
3.2 Contact form
3.3 Chatbot
3.4 Newsletter
3.5 Google Analytics
3.6 Map service
3.7 Pageflow
3.8 YouTube Videos
4. Links to third-party websites
5. Cookies
6. Recipients of personal data
7. Data processing in third countries
8. Retention period
9. Rights of data subjects
10. Commissioner for data protection
11. Update status

TIPIK

Tipik has a Data Protection Office (DPO), responsible for defining, managing and supervising that TIPIK complies with privacy regulations. It also provides training on personal data processing.

	Data is stored on servers located in Denmark, accessible only by Tipik's staff through a secured VPN. **ACA** ACA has a Data Protection Officer (DPO), responsible for defining, managing and supervising that ACA staff complies with the privacy regulations. Organisational measures include appropriate access rights. Data is stored on servers, based in the EU/EEA, accessible to ACA staff only, via a personal password.

14	**Information to data subjects / Data Protection Notice (DPN)**
	
	A Data Protection Notice will be provided by the Consortium to the relevant data subjects before any data processing activity which is in scope of this record. A Powerpoint slide regarding the recording will also be displayed during the events.
	
	- A Data Protection Notice / privacy statement will be provided to all data subjects prior to carrying out any data processing activities.
	- A PPT slide will be used at events to inform about the recording of events.
	- The Data Protection Notice will be included in event registration forms:
	  o The participants need to tick a box before completing their registration to acknowledge that they have read the Data Protection Notice which is displayed in PDF.
	  o In the case of individual interviews, the interviewees will receive the DPN (or be redirected to the DPN on the platform) and will be invited to give their consent for their name to be published when relevant.
	- The Data Protection Notice will be provided via a permanently visible link on the Community of Practice platform.