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 *2024-06*

In accordance with Article 31 of the Regulation

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.*

Missions in EACEA	
1	**Last update of this record (where applicable)**
	N/A as this is a new record (first version)
2	**Short description of the processing**
	This processing operation is to allow the organization of the professional travel (mission) and accommodation of EACEA staff and the payment of the resulting costs.
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): EACEA.B.4.003 EACEA-MISSIONS@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)**
	Not applicable
6	**Name and contact details of processor (where applicable)**
	NEO/AMEX NEO is the IT platform used by the staff to order the travel tickets AMEX is the external services invoicing the travel costs to EACEA Those are contractors if the EC (PMO acts as a separate controller)
7	**Purpose of the processing**
	The purpose of this processing operation is to allow the organization of the travel, accommodation of EACEA staff during missions and the payment of the resulting costs (and related reporting activities as part of the entire cycle of actions/tasks to the missions). To ensure the most cost-effective management of the missions of its staff, the EACEA relies on external service providers contracted by the EC. The mission management activity is broken down into a number of internal operations and other operations that are performed by the selected contractors. These contractors are: □ the travel agency responsible for issuing tickets, making hotel / car reservations; □ the organization responsible for issuing the credit card; □ the insurance / assistance company in charge of covering in a complementary way the head of mission in the event of illness / accident, or any other risk defined by the police coming on mission; □ car rental companies that can be used for missions; □ transport companies (airlines, railways, taxi etc); □ hotels, and / or other "assimilated" accommodation options (bed and breakfast, apart-hotel); □ and any other body that may be called upon to intervene by the specificity of the mission.
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 ☐ Applicants ☐ Relatives of the data subject ☐ Complainants, correspondents and enquirers ☐ Witnesses ☐ Beneficiaries ☐ External experts ☐ Other, please specify:
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

☐ 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

☒ concerning leave and absences

☒ concerning missions and journeys

☐ 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: Title, surname, first name, date of birth, login, number of staff, number per id, assignment, place of assignment, office address, business telephone number, professional email address, credit card number, place(s) mission and transit, the estimated time of departure and return at the duty station, the means of transport used, the name of the hotel, the invoice(s), the start and end times of the professional engagements at the mission site, the agent's bank account number, the budget line to which the mission will be charged, the MIPS mission number and the confirmation number generated at the moment of signature for approval by the authorizing officer.

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)**
	The data collected for mission management - are kept for a maximum of 10 years in line with the CRL (point 12.3.1). Once the legal deadline has expired, the file is deleted. **Is any further processing for historical, statistical or scientific purposes envisaged?** ☐ yes ☒ no **If yes, indicate the further retention time:** N/A According to the EC record - DPR-EC-00990.3, documents sent to the PMO as a separate controller, are stored and archived in the Office's archiving premises. Once the mission has been paid, staff members sent on mission may destroy the original paper documents unless they wish to contest the statement of account, in which case the original documents will be required to lodge a complaint under Article 90 (2) of the Staff Regulations. Once the statutory deadline has expired, the paper and digital file are destroyed. Digitized and paper files will only be destroyed by DIGIT at the express request of PMO
11	**Recipients of the data**
	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: -Commission services: - PMO Unit in charge of missions (as separate controller https://ec.europa.eu/dpo-register/detail/DPR-EC-00990) - DG BUDG for ABAC, etc. - External contractors of the EC as listed above (processors, see above) and other external entities (insurance, travel agency, transport companies, hotels, etc) for mission execution 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 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).
	Are there any transfers of personal data to third countries or international organisations? If so, to which ones and with which safeguards?
	The contractor/ travel agency providing the service (AMEX-GBT) may be required to transmit data concerning the travel agent / authorised traveller to a country outside the EU for his/her mission. As travel is inherently global, transfers of personal data outside of EU and EEA could occur, depending on the travel location. In order to organise travel, booking information is shared with airlines, hotels and other travel suppliers around the world. - Transfers of the travel agency within its 'corporate family' are based on Art. 48(2)(d) of the Regulation - Binding Corporate Rules (BCRs); - Transfers are also based on Article 50 of the Regulation since 'the transfer is necessary for - important reasons of public interest; - the performance of a contract between the data subject and the entity of the controller or the implementation of pre-contractual measures taken at the data subject's request.

	According to the EC record: DPR-EC-00990.3 ' The conditions for transferring data outside the EU are laid down in specific agreements with service providers (AMEX Global Business Travel, etc).' Travels to countries subject to an adequacy decision may be based on such decision if the related conditions are fulfilled .
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: 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: State of the art technical cybersecurity measures are implemented in the corporate systems, according to the security needs. Those measures are in constant evolution. EACEA's contractors are bound by a specific contractual clause for any processing operations of the data on behalf of the Agency, and by the confidentiality and data protection obligations. deriving from the application of the Regulation and the General Data Protection Regulation in the EU Member States ('GDPR' Regulation (EU) 2016/679).
14	**Information to data subjects / Data Protection Notice (DPN)**
	The DPN will be made available to the data subjects via the internal EACEA SharePoint on missions.