EUROPEAN EDUCATION AND CULTURE
EXECUTIVE AGENCY (EACEA)

EACEA.R2 - Budget and Control

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 **06-2021**

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.*

	Ex-post audits
1	**Last update of this record (where applicable)**
	N/A
2	**Short description of the processing**
	One of the tasks of the ”Performance, Audit and Internal Control team of unit R2 is to coordinate the ex-post audits (on-the-spot) of grant projects managed by the EACEA.
	Part 1 - Article 31 Record
3	**Name of the Controller** **Unit and/or function of person acting on behalf of the Controller**
	Controller: European Education and Culture Executive Agency Unit: Head of Unit R2 budget and Control eacea-R2-audit@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)**
	Framework contract in cascade for audit services with different audit companies: 1. Framework contract 2021-AUDFWC-01DL signed with Deloitte Bedrijfsrevisoren/Reviseurs D'entreprises Gateway Building, Luchthaven Nationaal 1J 1930 Zaventem Belgium 2. Framework contract 2021-AUDFWC-02BDO signed with BDO LLP Limited Liability Partnership 55 Baker Street, W1U 7EU, London UK 3. Framework contract 2021-AUDFWC-03PKF signed with PKF LITTLEJOHN LLP Limited Liability Partnership 1 Westferry Circus, Canary Wharf, GB-London E14 4HD
7	**Purpose of the processing**
	The ex post audits of grant agreements and decisions aim at verifying beneficiaries' or subcontractors' or third parties' compliance with all contractual provisions (including financial provisions), in view of checking that the provisions of the grant agreement or decision were properly implemented and in view of assessing the legality and regularity of the transactions underlying the implementation of the Union budget. Ex-post audits are mainly outsourced to external audit firms but could be carried out directly by EACEA staff ("own-resource-audits") .
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 ☐ Contractors ☒ Other, please specify: Staff members and subcontractors of beneficiaries or any other natural persons involved in the matter being audited.
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 ☒ 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: names, function & grades, contact details and addresses (phone number, email addresses, personal and professional address)_____ ***b) Categories of personal data processing likely to present <u>specific risks:</u>*** ☒data relating to suspected offences, offences, criminal convictions or security measures: processing of such data is purely incidental, but might take place in case of exclusion as provided for by Financial Regulation ☐ 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 Auditors might have access to such data but they are disregarded as they are not the scope of their audit. ***d) Specify any additional data or explanatory information on the data being processed, if any:*** Performance, Audit and Internal Control sector team of unit R2 keeps two categories of data, i.e. a) project data (e.g. project number and type, global budget, etc.) and b) data of beneficiary (such as address of the organisation, name, contact details of the persons responsible for the projects, personal data linked to audit findings) The categories of data contained in documents may vary depending on the nature of the project and the matter being audited.
10	**Retention time (time limit for keeping the personal data)**

	Data are retained for 10 years starting from the closure of the annual audit plan file where audit information are stored. This isin compliance with the Common Retention List (CRL)– Commission Decision SEC/2019/900 of 09/07/2019, Annex 1, point 7.1.3. Data are retained for 10 years after the annual audit plan file is closed on condition that no contentious issues occurred; in this case, data will be kept until the end of the last possible legal procedure. After that, they may be transferred to the Historical Archives of the EC (as indicated in the Commission Common retention list). **Is any further processing for historical, statistical or scientific purposes envisaged?** ☒ yes ☐ no **If yes, indicate the further retention time:** After the 10 years retention period, according to the Commission Common retention list, files can be chosen for preservation, the remainder is destroyed. The files identified for preservation are transferred to the Commission's Historical archives;
11	**Recipients of the data**
	- Designated staff of EACEA such as: • Financial/project/legal officers in EACEA; • Authorised financial officers of unit R2 of EACEA; • Authorised Officers by (sub-) Delegation in EACEA (Director, Heads of Department, Heads of Unit , Heads of sector); - External auditors (processors) acting on behalf of EACEA, and their subcontractors if any; - European Commission, such as DGs, Commission services in charge of ex-post controls, IAS auditors In case of control or dispute the bodies in charge of a monitoring and/or inspection task in accordance with EU law (OLAF, European Court of Auditors, Ombudsman, EDPS, Internal Audit Service of the Commission, etc.).Data may be transferred to EU and national public authorities in the framework of a particular inquiry in accordance with Union or Member State law .e.g. OLAF, EPPO, Internal Audit Service of the Commission, European Court of Auditors, Ombudsman, EDPS, IDOC, national authority, the European Court of Justice or a national judge etc.) as well as to the lawyers and the agents of the parties in case of a legal procedure,
12	**Are there any transfers of personal data to third countries or international organisations? If so, to which ones and with which safeguards?**
	Personal data can be transferred to the UK based on the Commission Implementing Decision C(2021) 4800, pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom, to the extent that the adequacy decision is respected by the recipient and remains valid. Furthermore, EACEA can authorise transfers into third countries other than UK which do not have adequacy decisions in case the audited entity is based into a third country and the contractor needs to recruit a local auditor to partly or fully carry out the audit. Such transfers will be based on a derogation of Article 50(b) (transfer necessary to perform a contract between data subjects and the controller), and 50(1)(d) (transfer is necessary for important reason of public interest recognised by EU law , which in this case is the Financial Regulation).
13	**General description of the technical and organisational security measures**
	Organisational measures include appropriate access rights and access control. Access to the IT tools is given on need-to-know basis to a limited number of persons within the ex-post sector. The external auditor's contract includes a confidentiality clause, and data protection provisions for processors. **Technical measures** include the use of secure equipment (e.g. locked cupboards) and IT-tools (including secure connections, firewalls, etc.). 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. In this context a specific 'Information Security Technology Plan' is reviewed annually with a view to describe the implementation of the above rules and guidelines in EACEA. The procedures set out in the document must be applied to the Agency's IT systems to ensure the security of the stored data and they are based on the European Commission's standards on security. The Server Rooms of the Agency are equally protected and locked.
14	**Information to data subjects / Privacy Statement**
	Privacy statement will be published on the website of the Agency. The link to it will be included in the announcement letter.