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 **07/2021**

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*
☒ *Migration from notification to record.*

Anti-Fraud procedure for analysis and signalling suspicions of irregularities and/or fraud to OLAF	
1	**Last update of this record (where applicable)**
	Ares(2013)2711352 - 19/07/2013
2	**Short description of the processing**
	Management of suspicions of irregularities/fraud in i) procurement contracts, projects, at the selection and/or implementation stage, by applicants, beneficiaries, experts, subcontractors from all programmes managed by EACEA should it be legal entities or natural persons; ii) EACEA staff Most of the data relates to public or privates companies and organisations but it includes also the names, functions, contact data and activities to be implemented (application) or implemented (reports) by personnel, experts and (sub)contractors involved in the projects or by service providers.

	The origin of the suspicion can be a desk review, an audit, a denunciation made to EACEA by anyone (inside or outside the applicant/beneficiary partnership), anonymously or not, at OLAF request or at request of national authorities in charge of investigating/prosecuting fraud allegations (police, antifraud office, financial or judicial authorities, etc). For suspicions received/discovered by EACEA, if the internal preliminary controls leads to a transmission to OLAF, all documents related to the suspicious applications and/or projects (consultation including personal data) concerned are transmitted to OLAF, after prior parent DG's consultation. In case of OLAF/EPPO requests, all requested documents and information related to the suspicious applications and/or projects concerned are gathered and transmitted to OLAF/EPPO; In case of requests by Judicial National authorities, there is a prior consultation of the parent DGs, OLAF and EACEA DPO.
Part 1 - Article 31 Record	
3	**Name of the Controller** **Unit(s) and/or function of person acting on behalf of the Controller** The Head of Unit R2 Budget and Control: EACEA-R2-ANTI-FRAUDE@ec.europa.eu Administrative address: J-59 07/061 Postal address: Education and Culture Executive Agency, Avenue du Bourget 1, BOUR, BE-1140 Brussels.
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)** Not applicable
7	**Purpose of the processing** The purpose of this processing operation is to : i) Assess allegations of fraud and analyse information about potential fraud and financial irregularities in order to determine whether there are grounds to transmit the information to the European Anti-Fraud Office (OLAF) in order to safeguard EU financial interest and/or prevent or tackle possible irregularities; ii) Answer to requests received from other EU Institutions and bodies (e.g. Commission DGs, EPPO, OLAF) or national authorities (police, antifraud office, financial or judicial authorities etc) for their investigations and controls.

8	**Description of the categories of data subjects**
	☒ Agency staff (Contractual and temporary staff in active position) ☒ Contractors providing goods or services ☒ Applicants ☒ Complainants, correspondents and enquirers ☒ Witnesses ☒ Beneficiaries ☒ External experts ☒ Contractors ☒ Other, please specify: whistle-blowers, informants, interns and interim staff of the Agency,
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 [contract, salary slip, time sheets and proof of salary payment, any other mean to prove the amount paid) ☒ concerning recruitment and contracts [documents linked to the recruitment procedure, contract of staff working on projects, experts or (sub)contractors ☐ concerning the data subject's family ☒ concerning the data subject's career [CV s qualifications when relevant to justify its relevance to the costs charged on projects] ☒ concerning leave and absences ☒ concerning missions and journeys [hotel bills, transport tickets (flights, trains, cars, list of presence to events, seminars/conference materials etc) ☒ concerning social security and pensions [salary payslips and other documents that allow the control of the daily rate charged on projects] ☒ concerning expenses and medical benefits ☐ concerning telephone numbers and communications ☒ concerning names and addresses (including email addresses) [Dun Bradstreet database to find back beneficiaries and check if the companies still exists] ☐ 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:*** _all justifying documents related to the costs charged under projects (staff costs, travels, accommodation, activities/deliverables, equipment, subcontractors, conference/events/festivals/trainings etc) can be requested._____
10	**Retention time (time limit for keeping the personal data)** The **retention period** of personal data is: a) Cases analysed in EACEA but **not transferred to OLAF**: • In the absence of measures taken by the Authorising Officer ("AO"): 3 years after dismissal, to be calculated from the date of the communication of the dismissal by the anti-fraud coordinator to the operational unit concerned. • If the AO has adopted measures: 5 years after the end of the implementation of the last of those measures. b) Cases **dismissed by OLAF or closed without recommendations**: • In the absence of measures taken by the AO: 3 years after dismissal • If the AO has taken parallel actions: 5 years after implementation of those measures. c) Cases **closed by OLAF with follow-up or recommendations**: • 5 years after implementation of the actions recommended by OLAF • If the AO has taken additional or complementary measures: 5 years after implementation of both set of actions • In the event that a national police, judicial or anti-fraud investigation is in progress, the time limit of 5 years begins to run from the date the Agency is informed by OLAF of the closure of this investigation In case the retention period expires when an inspection task (e.g. audit) or a judicial proceeding related to the file is ongoing, the personal data is retained for the time necessary to the finalisation of such inspection tasks or settlement of the judicial proceeding. **Is any further processing for historical, statistical or scientific purposes envisaged?** ☐ yes ☒ **no** We do **not** have to further process/keep the personal data for public interest, scientific or historical research purposes or statistical purposes. Only non-personal data related to

	organisations (type of organisation, country, programme concerned by fraud are used for statistical purposes (risk assessment) **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**
	• Inside EACEA: R2 Anti Fraud coordinator, staff from the operational unit(s) managing the concerned projects, Management (HoU, HoD, Dir), legal sector (unit B4), B5 (for financial issues) R1 (for staff or access to documents); • Outside: Parent DGs, Internal Audit Service, European Commission services if the request concerns documents of the European Commission where the contribution from or re-attribution to the EC is necessary, external auditors, European Court of Auditors (ECA); EUI services for a particular investigation/visit/ inspection (e.g. OLAF, European Ombudsman, EDPS, IDOC), EPPO, European Court of Justice; competent national authorities such as National authorities (at their request)lawyers appointed by EACEA or the Commission.
12	**Are there any transfers of personal data to third countries or international organisations? If so, to which ones and with which safeguards?**
	Documents related to suspicious projects and/application can be requested by and transferred to National authorities (judicial, fiscal, police) when EU funds are subjects to potential fraud under investigations. The third countries where the data can be transferred can be anywhere, depending on the country of establishment of the recipient of EU funds where the fraud investigation takes place. Safeguards: Such transfer is decided and made by OLAF in accordance with the legal framework. In case the third country of destination is not covered by an adequacy decision or in absence of adequate safeguards in place (e.g. administrative arrangement), the transfer might take place based on a derogation under Article 50-1 of Regulation 2018/1725, in particular if necessary for important reason of public interest (art 50-1-d), or for the establishment, exercise or defence of legal claim (art 50-1-e).
13	**General description of the technical and organisational security measures**
	Organisational measures include appropriate access rights and access control. **Internal** The Anti-Fraud procedure contains in its chapter VI specific rules on confidentiality which are reminded i) at the occasion of the treatment of each file (though email exchanges, skype meetings etc) as it can relate to any project managed by different staff members, ii) at the occasion of trainings. Agents are required to transfer new suspicious cases or for the follow up of ongoing cases to use exclusively encrypted emails and addressed to agents only on a "need to know basis". **External** Data transfer – confidentiality clause:

	Where personal data are transferred to other EU institutions and bodies), specific safeguards are taken. • In all e-mails sent by the anti-fraud coordinator, a reference is made to draw attention to the fact that the data transferred falls within Article 4(2) of Regulation 2018/1725 on the protection of personal data. The same reference can be found on the template of the transmission note from the Agency to OLAF concerning potential cases of irregularity/fraud: *"The transfer of personal data to you is performed under the regime of Regulation 2018/1725 on the protection of natural persons with regard to the processing of personal data by Union Institutions, bodies, offices and agencies and of the free movement of such data and repealing Regulation (EC) 45/2001 and Decision N° 1247/2002/EC. Accordingly, as the Controller of the personal data hereby transmitted, you are responsible for ensuring that they are used only for the purpose for which they are transmitted. Processing in a way incompatible with that purpose is contrary to the conditions upon which the data has been transferred to you. Furthermore, according to Article 4(2) of Regulation 2018/1725, you are required as the Controller of the personal data concerned to ensure that paragraph 1 of the same Article is complied with, together with all other obligations of the Controller including informing the data subjects (Article 16) and security of the processing (Article 33)."* Cases transmitted to OLAF are sent through encrypted IT tools or in 2 sealed envelopes **Technical measures include the use of secure equipment (e.g. locked cupboards) and IT-tools (including secure connections, firewalls, etc.).** <u>Data storage security</u> The electronic data is stored on the Anti-fraud (AF) coordinator's special drive with very limited access (AF coordinator and R2 HoU) and in subfolders under the functional mailbox (EACEA-R2-ANTI-FRAUDE) with the same very limited access. Paper files are kept in locked cupboards. As appropriate, the documents produced and/or received by the Anti-fraud coordinator are registered and classified through the standard Commission's system (ARES). In order to protect the confidentiality of the information, the documents submitted or received are always registered as "handling restriction" in ARES and without attachment. OLAF documents (requests, reports, notification of dismissal/opening investigations) are not dispatched to the units and are kept in the AF Coordinator secured folders.
14	**Information to data subjects / Privacy Statement**
	In order to ensure information of the data subjects in accordance with Articles 15 and 16 of the Regulation 2018/1725 the privacy statement is published on: EACEA's external website: https://www.eacea.ec.europa.eu/about-eacea/data-protection_en#ecl-inpage-1044 EACEA's internal intranet page: https://myintracomm.ec.europa.eu/dg/eacea/mydailywork/anti-fraud/Pages/cooperation.aspx In accordance with Article 25 of Regulation (EU) 2018/1725, in matters relating to the operation of EU institutions and bodies, the latter can restrict certain rights of individuals in exceptional circumstances and with the safeguards laid down in that Regulation. Such

	restrictions are provided for in internal rules adopted by EACEA and published in the Official Journal of the European Union (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021Q0317%2801%29)
	
	Besides this, the following information is provided to data subjects:
	
	• Specific Privacy statements exists for grant and procurement procedures as well as for audits launched by the Agency.
	
	• The model agreement/decision/contract signed between the Agency and its counter parts contains in its General Condition a number of provisions informing its signatory(ies):
	
	  • A provision allowing the Agency and/or the Commission to carry out technical and financial checks, audits &/or evaluations in relation to the use of the grant, and an obligation for the beneficiary/contractor to provide any information requested in that respect.
	  • A provision allowing OLAF/EPPO to carry out checks and the Court of Auditors to carry out audits.
	
	When the Authorising Officer adopts precautionary measures as a result of a suspicion of fraud/irregularity (OLAF recommendation or AO measures), although the concerned party is not informed of the investigation itself, he/she is informed by a motivated decision of the measures taken as a result of this investigation which might affect its rights. The AO will thus communicate to the concerned party the measures taken, such as a request or mobilisation of a financial guaranty, the suspension of a payment, the termination of a grant/contract, the launching of a recovery, etc.
	
	However, in order to protect the confidentiality of the investigation, the AO will not justify its decision on the existing suspicion but on the element having led to this state of suspicion.