



## **Anti-Fraud procedure for signalling suspicions of irregularities and/or fraud**

### **Privacy Statement**

The European Education and Culture Executive Agency ("EACEA") is committed to preserving your privacy. All personal data are dealt with in accordance with Regulation (EU) No 2018/1725 on the protection of personal data by the Union institutions, bodies, offices and agencies<sup>1</sup> ("the data protection regulation").

The following Privacy statement outlines the policies by which the EACEA collects, manages and uses the personal data of the concerned individuals within the **signalling of suspicions of irregularities and/or fraud**

#### **Who is responsible for processing your personal data (data controller)?**

The controller is the European Education and Culture Executive Agency, BE-1049 Brussels

The person designated as being in charge of the processing operation is the Head of Unit R2 Budget and Control

Email: [EACEA-R2-ANTI-FRAUDE@ec.europa.eu](mailto:EACEA-R2-ANTI-FRAUDE@ec.europa.eu).

#### **1. Which personal data are processed?**

The **categories of personal data** processed may include the following:

- Name and contact details: address, e-mail, phone numbers, pictures;
- Position and responsibilities within the concerned entity and in other entities;
- Personal data contained in the proposal/offer, the grant agreement, the procurement contract, progress, interim and final reports, audit certificate, deliverables and/or justifying documents required by the grant agreements and contracts. These may be statutes, time sheets, payslips, employment contracts, travel costs, accommodation costs, procurement procedure, bank statements etc.;
- Information on the conduct of the person giving rise to possible irregularities. Documents used as evidence may be job descriptions, CVs, information on social networks' profiles etc;
- Personal data which appear in legal entity and bank account files;

---

<sup>1</sup> 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 Text with EEA relevance, OJ L 295, 21.11.2018, p. 39.

- Personal data on other grants/contracts managed by EU Institutions and bodies or Agencies involving the entity or the person concerned;
- Name and contact details: address, e-mail, phone numbers;
- Personal data which appear in legal entity and bank account files (information available in the corporate financial management system used by the Agency);
- CV, job description;
- Information on the conduct of the person giving rise to possible irregularities;
- Appraisal reports and probationary reports if they provide relevant information and evidence of the past and current behaviour under scrutiny.

### **For which purpose do we process your data?**

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.

EACEA does **not** have to further process/keep the personal data for public interest, scientific or historical research purposes or statistical purposes. Only data related to organisations (type of organisation, country, programme concerned by fraud are used for statistical purposes (risk assessment)).

### **2. Where the data is collected from?**

From the applicants: At the application stage, all data are coming from the applicants participating to call for proposals: they fill in an “*application form*” and download documents related to their entity, their co-beneficiaries and the project they propose to implement;

From the (co)-Beneficiaries: during the implementation stage, all data are coming from the (co)-beneficiaries participating to the implementation of the selected projects: they fill in pro-forma interim and/or final reports and transmit documents contractually due, related to the project they have implemented (deliverables and audit certificates, justifying documents;

From the contractors that apply to call for tenders: they transmit all documents related to their entities and their offer (terms of references, budget, company’s accounts, and possibly references proving their capacity to do it).

From the staff: when they are recruited or at a later stage, in case of change of their status or claim for repayment of costs (mission, medical claim etc).

Furthermore, personal data can be collected from outside sources of information such as articles in newspapers or other information (exchange of emails etc) transmitted to EACEA by denunciators.

### **3. Who has access to your personal data and to whom is it disclosed?**

The data processed will not be communicated to third parties, except where necessary for the purposes outlined above. Access to your personal data may be given on a need-to know basis to the following recipients:

- 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);
- External services: European Commission Parent Directorate-Generals, Internal Audit Service, European Commission (EC) services if the request concerns documents of the EC where the contribution from or re-attribution to the EC is necessary, external auditors, European Court of Auditors (ECA); European institutions 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.

In case of control or dispute, the bodies charged with a monitoring or inspection task in application of Union law (e.g. Internal Audit Service, European Commission, OLAF, EU Courts etc.).

#### **Transfers outside the EU:**

Documents related to suspicious projects and/application can be requested by and transferred to non-EU/EEA 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).

### **4. How long do we keep your 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.

**5. What are your rights concerning your personal data and how can you exercise them?**

Under the provisions of the data protection regulation, you have the right to:

- Request to access the personal data EACEA holds about you;
- Request a rectification of your personal data where necessary;
- Request the erasure of your personal data;
- Request the restriction of the processing of your personal data;
- Request to receive or to have your data transferred to another organization in commonly used machine-readable standard format (data portability).

You can exercise your rights by writing to the Agency at the attention of the controller at the email address indicated above.

As this processing of your personal data is based on point of Article 5(1)(a) of the data protection regulation, please note that you have the right to object to processing of your personal data on grounds relating to your particular situation under the provisions of Article 23 of the data protection regulation.

You should be informed that, by virtue of Article 25 of the data protection regulation, one or several of these rights might be restricted for a temporary period of time inter alia on the grounds of prevention, investigation, detection and prosecution of criminal offences or other ground.

Such restriction is provided for in the Internal rules adopted by EACEA on 22 October 2020 and published in the Official Journal of the EU: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32021Q0317%2801%29>

Any such restriction will be limited in time, proportionate and respect the essence of the above-mentioned rights. It will be lifted as soon as the circumstances justifying the restriction are no longer applicable. You will receive a more specific data protection notice when this period has passed.

As a general rule, you will be informed on the principal reasons for a restriction unless this information would cancel the effect of the restriction as such.

You have the right to make a complaint to the EDPS concerning the scope of the restriction.

## **6. Your right to have recourse in case of conflict on any personal data issue**

In case of conflict on any personal data protection issue, you can address yourself to the Controller at the above-mentioned address.

You can also contact the Data Protection Officer of EACEA at the following email address: [eacea-data-protection@ec.europa.eu](mailto:eacea-data-protection@ec.europa.eu).

You may lodge a complaint with the European Data Protection Supervisor at any time: <http://www.edps.europa.eu>.

While individuals concerned may lodge a complaint with the European Data Protection Supervisor at any time (website <http://www.edps.europa.eu>; e-mail: [edps@edps.europa.eu](mailto:edps@edps.europa.eu)), it is recommended to try to resolve the conflict with the Controller or the Agency's Data Protection Officer before filing such a complaint.

## **7. On which legal basis are we processing your personal data?**

Article 5(1)(a)-(e) of the Regulation giving the legal basis to this processing:

- (a) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body, including processing of personal data necessary for the management and functioning of the Union Institutions or bodies [Recital 22]
- (b) processing is necessary for compliance with a legal obligation to which the controller is subject.

### **Legal basis:**

- (a) Regulation (EC, Euratom) No 883/2013 of the European Parliament and of the Council concerning investigations conducted by the European Anti-Fraud Office (OLAF), and repealing Regulation (EC) No 1073/1999 of the European Parliament and of the Council and Council Regulation (Euratom) No 1074/1999, OJ L 248/1, 18.9.2013;
- (b) Commission Decision of 10.7.2020 - C(2020) 4584 amending Decision C(2018) 5119 on the internal procedure provisions for the recovery of amounts receivable arising from direct management and the recovery of fines, lump sums and penalty payments under the Treaties;
- (c) The Commission Implementing Decision 2021/173 establishing the European Education and Culture Executive Agency;
- (d) The Commission Decision C(2021)951 and its annexes delegating powers to EACEA for the management of programmes in the MFF 2021-2027.
- (e) Administrative arrangements on co-operation and a timely exchange of information between the European Commission and the European Anti-Fraud Office (OLAF), 4.12.2018 and General Memorandum of Understanding between the Agency and its parent DGs;
- (f) Interinstitutional Agreement between the European Parliament, the Council of the European Union and the Commission of the European Communities concerning internal investigations by the European Anti-Fraud Office (OLAF), OJ L 136/15, 31.5.1999;
- (g) EACEA's Steering Committee decision of 9/6/2006 laying down internal rules to prevent fraud, corruption and any illegal activity detrimental to the Communities' interest.

(h) Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Union, Articles 11 to 26a on staff duties.