



EUROPEAN COMMISSION  
RESEARCH EXECUTIVE AGENCY

## RECORD OF PERSONAL DATA PROCESSING ACTIVITY

*In accordance with Article 31 of the Regulation (EU) 2018/1725 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 (Regulation), individuals whose personal data are processed by the Research Executive Agency (REA or 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 activities.*

Record No: 40  
Created on (date): XX December 2019  
Last update (date):

### NAME OF THE PROCESSING ACTIVITY

Whistleblowing procedure in REA (handling confidential whistleblowing reports)

## **1. MANDATORY RECORD UNDER ARTICLE 31 OF THE REGULATION**

### **1.1. Name and contact details of controller**

The controller is the Research Executive Agency (REA). For organisational reasons, the role of the data controller is exercised by Mr Marc BELLENS, Head of Department Administration, Finance and Support Services. The controller may be contacted via email address: [marc.bellens@ec.europa.eu](mailto:marc.bellens@ec.europa.eu).

### **1.2. Name and contact details of the Data Protection Officer (DPO)**

Ms Maria Francisca BRUNET COMPANYY

([REA-DATA-PROTECTION-OFFICER@ec.europa.eu](mailto:REA-DATA-PROTECTION-OFFICER@ec.europa.eu)).

### **1.3. Name and contact details of joint controller (where applicable)**

Not applicable

### **1.4. Name and contact details of processor (where applicable)**

Not applicable

### **1.5. Purpose of the processing**

In the frame of the processing operation for whistleblowing in REA, personal data is collected and/or processed based on Articles 22a (internal whistleblowing) of the Staff Regulations.

Having procedures for raising concerns about fraud, corruption or other serious wrongdoing is relevant for all responsible organisations and for the people who work there. While good internal control systems can reduce the probability of something going seriously wrong, this risk can never be reduced to zero. Where this risk materialises, the first people to realise or suspect the problem will often be those who work in or with the organisation. Yet unless the culture is one where employees believe that it is safe and accepted that such concerns are raised, the risk is that people will stay silent. This denies the organisation an important opportunity to detect and investigate the concern, to take any appropriate action and to protect its assets, integrity and reputation. The most effective way to encourage staff to report concerns is to provide assurance of protection of their position. Clearly defined channels for internal reporting as well as safe and accepted routes through which staff may raise concerns outside the organisation as an option of last resort should be in place. Viewed in this way, having whistleblowing procedures and whistleblower protection in place is simply a question of good management and a means of putting into practice the principle of accountability. They contribute to improving the diligence, integrity and responsibility of an organisation. It is against this background that rules on whistleblowing were adopted and included in the Staff Regulations (Articles 22a and 22b)<sup>1</sup> in 2004. They complement the general principle of loyalty to the European Union, the obligation to assist and tender advice to superiors (Article 21) as well as the rules on how to deal with orders which are considered to be irregular or likely to give rise to serious difficulties (Article 21a).

While these rules have already triggered a number of significant investigations by the European Anti-Fraud Office (OLAF), some staff may be reticent to make full use of the whistleblowing procedure, because of a fear of negative repercussions on their reputation or career. As part of the REA's duty to have regard for the interests of staff members ('devoir de sollicitude'), it is necessary to ensure that members of staff who report serious wrongdoings or concerns in good faith are afforded the utmost confidentiality and greatest degree of protection against any retaliation as a result of their whistleblowing. As whistleblowing arrangements are widely recognised as an important tool to detect fraud, corruption and serious irregularities, it is important that staff fully understand the types of situations where the obligation to 'blow the whistle'

applies, and to whom they should address their concerns. Providing guidance on this issue is part of the REA's overall ethics policy, which aims inter alia at clarifying the rules regarding professional ethics in the REA.

Thus, the purpose of the processing operation in REA is to:

- Provide safe channels to staff to report fraud, corruption or other serious wrongdoings in REA;
- Offer guidance and support to potential whistleblowers;
- Provide feedback to the whistleblower;
- Ensure the proper follow-up on the reported alleged facts;
- Ensure protection of the whistleblower and the person against whom the allegation is made and any other natural person mentioned in the report/involved in the case.

The whistleblowing procedure/channels are not used for reporting:

- Information already in the public domain (for example: newspaper articles, publicly available audits);
- Unsubstantiated rumours and hearsay;
- Matters of a trivial nature;
- Disagreements over legitimate policy;
- Information not linked to the performance of one's duties.
- Personnel issues where staff have a personal interest in the outcome;
- Harassment claims and personal disagreements or conflicts with colleagues or hierarchy;
- Abusive disclosures (repeated disclosures of alleged facts aimed merely at paralysing a service);
- Malicious, frivolous or potentially defamatory disclosures (i.e. false or unverifiable accusations with the aim of harming another person's integrity or reputation).

#### **1.6. Legal basis for the processing**

- Articles 317 and 325 of the Treaty on the Functioning of the European Union (TFEU) regarding the protection of the financial interests of the Union and the fight against fraud affecting these interests;
- The Staff Regulations of Officials of the European Union ('Staff Regulations') and the Conditions of Employment of Other Servants of the European Union (CEOS), laid down by Council Regulation (EEC, Euratom, ECSC) No 259/68, in particular Articles 22 of the Staff Regulations and Articles 11 and 81 of the Conditions of Employment of Other Servants of the European Communities;
- Regulation (EU, Euratom) 2018/1046 on the financial rules applicable to the general budget of the Union, repealing Regulation (EU, Euratom) No 966/2012 (2012 Financial Regulation);
- Regulation (EU, Euratom) No 883/2013 of the European Parliament and of the Council of 11 September 2013 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;

- Council Regulation (EC) No 58/2003 of 19 December 2002 laying down the statute for executive agencies to be entrusted with certain tasks in the management of Community programmes: Article 11 paragraph 6 and Article 18 paragraphs 1 and 3.
- Commission Regulation (EC) No 651/2008 of 9 July 2008 amending Regulation (EC) No 1653/2004 on a standard financial regulation for the executive agencies pursuant to Council Regulation (EC) No 58/2003 laying down the statute for executive agencies to be entrusted with certain tasks in the management of Community programmes;
- Commission Decision C(2013) 9418 final of 20.12.2013 on delegating powers to the Research Executive Agency with a view to performance of tasks linked to the implementation of Union programmes in the field of research and innovation comprising, in particular, implementation of appropriations entered in the general budget of the Union;
- Commission Implementing Decision 2013/778/EU of December 13th, 2013, establishing the Research Executive Agency and repealing Decision 2008/46/EC;
- Commission Decision C(2013)9418 of 20 December 2013 and its Annexes, which delegates powers around the performance of tasks relating to the implementation of programmes in the field of research and innovation. As of 1 January 2018, the Agency's mandate was extended by adding validation services for all grant management and procurement activities of the Commission (SEDIA project), as well as the management of projects that involve classified information (see Commission Decision C(2017)4900 of 14 July 2017).
- Communication from Vice-President Šefčovič to the Commission on Guidelines on Whistleblowing (SEC (2012) 679 final);
- Commission Decision of 27.02.2018 on giving the Commission's ex ante agreement to the adoption by agencies of implementing rules laying down guidelines on whistleblowing;
- Decision of the REA Steering Committee laying down implementing rules on whistleblowing (REA/SC (2019)2.3) of 15 October 2018;
- Communication on 29.4.2019 from the Commission to the European Parliament, the Council, the European Economic and Social Committee, the Committee of the Regions and Court of Auditors on the Commission Anti-Fraud Strategy: enhanced action to protect the EU budget - COM(2019) 196 final;
- Decision of the Steering Committee of the Research Executive Agency (REA/SC(2008)5 rev.1) of 20 February 2008 on measures to combat fraud and irregularities, concerning the terms and conditions for internal investigations in relation to the prevention of fraud, corruption and any illegal activity detrimental to the Communities' interests;

### **1.7. Categories of data subjects**

REA staff members (contract agents, temporary agents under Article 2 (f) of the CEOS and temporary agents under Article 2 (a) of the CEOS (officials on secondment), and, by extension, any external staff working intra muros (NB: they are not bound by the Staff Regulation), in their role of:

- Involved person allegedly committing wrongdoing; or
- Witness; or

- Third party mentioned in whistleblowing report; or
- Whistleblower: staff member reporting the alleged facts.

### 1.8. Categories of personal data

The whistleblowing report and the documents issued in the procedure may contain:

- For the whistleblower: first name and last name, function and place of employment / administrative address, email.
- For the person allegedly committing wrongdoing: first name and last name, function and place of employment, email, any other data necessary for the demonstration of the wrongdoing.
- For the witness: first name and last name, function and place of employment, any other data necessary for the justification of his/her quality as a witness.
- For the third party: first name and last name, function and place of employment, any other data contained in the report.

### 1.9. Retention time (time limit for keeping the personal data)

Following the internal whistleblowing procedure, we keep the data for 5 years as from the date of the decision about the follow-up to give to the whistleblowing report.

Is any further processing for historical, statistical or scientific purposes envisaged? **No**

### 1.10. Recipients of the data

Who will have access to the data within the Agency?

The whistleblower can send his/her written report to any person whom he/she considers relevant: from the immediate superior to the Director of the Agency. During the handling of the report, the first recipient can (it is not mandatory) involve:

- the Director of the Agency;
- the head of department "Administration, Finance and Support services";
- the head of sector "Legal affairs, Internal Control and Reporting";
- the REA Ethics correspondent;

Who will have access to the data outside the Agency?

- As a follow-up to the handling of the whistleblowing report, the information reported by the whistleblower can be transferred to OLAF. The necessity for transferring the personal data to OLAF is assessed on a case-by-case basis.

### 1.11. Transfers of personal data to third countries or international organisations

Are there any transfers of personal data to third countries or international organisations? **No**

### 1.12. High-level description of security measures

The registration and filing of the documents follow particular rules. Data in electronic format is stored on the REA or European Commission servers (limited access) and only metadata is stored on the servers (ARES) of the European Commission. Data/reports in paper format are stored in locked/secure cupboards.

### 1.13. Data Protection Notice

A Data Protection Notice (DPN) relevant to this data processing activity is available under the REA Intranet (Section "Data Protection").