EUROPEAN EDUCATION AND CULTURE
EXECUTIVE AGENCY (EACEA)

EACEA.R1 - People, Workplace and Communication

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 *01-2021*

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.*

Processing of personal data within the framework of the anti-harassment policy	
1	**Last update of this record (where applicable)**
	The relevant record was last updated in June 2021 (reference 01-2021).
2	**Short description of the processing**
	The processing aims at preventing and remedying cases of alleged harassment within the Agency during the informal procedure. The informal procedure aims at helping and protecting the alleged victim at an early stage.
Part 1 - Article 31 Record	
3	**Name of the Controller** **Unit(s) and/or function of person acting on behalf of the Controller**

	The controller is the European Education and Culture Executive Agency (EACEA). For organisational reasons, the role of the data controller is exercised by the head of Unit R1 ("People, Workplace and Communication") of the EACEA. The controller may be contacted via functional mailbox: EACEA-Harassment@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)**
	Not applicable
7	**Purpose of the processing**
	The processing aims at preventing and remedying cases of alleged harassment within the Agency during the informal procedure. The informal procedure aims at helping and protecting the alleged victim at an early stage. Presumed victims may also initiate the formal procedure under Article 24 of the Staff Regulations, which may be processed by IDOC. The personal data is collected and processed with the following aims: • to support and protect the victim; • to be able to refer cases to the relevant services; • to provide efficient and proper administration of cases to be solved as soon as possible; • to guarantee confidentiality and create conciliation; • to prevent cases; • to review request for help and any need for psychological support; • to identify recurrent cases and provide references for disciplinary actions where applicable; • to provide data for the formal procedure and to reply to the Ombudsman or legal authorities at the national or European level in the case that the complaint leads to a formal procedure. This processing does not cover the selection of Confidential Counsellors, which are covered by another record, nor the formal procedure per se, which is not handled by the Agency. Administrative inquiries are also covered by another specific record.
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: any persons potentially concerned, who could be alleged harasser, alleged victim, witness or other person implicated.
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: Administrative data of the alleged victim, alleged harasser, and/or witness or other person implicated e.g. name (surname at birth, current surname, forename), professional address (street, postcode, place, country), phone number (office & GSM), email address, unit/department, office number, date & place of birth, gender, nationality, etc. Relevant data for the harassment case collected through the Confidential Counsellors or directly from the alleged victim including the alleged working and personal situation of the data subject and of other implicated persons. ***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

	In particular, sensitive data relating to physical or psychological harassment might be processed, such asdata relating to health or sex life or sexual orientation or personal opinions or ethnic or racial origin may be processed in case of anti-harassment procedures. ***d) Specify any additional data or explanatory information on the data being processed, if any: -*** _____
10	**Retention time (time limit for keeping the personal data)**
	The Agency applies the principles and retention periods indicated in Common Retention List of the Commission[1]. *The Anti-Harassment Coordinator shall keep the files (both opening and closing files with the case) for a period of no more than five years after the outcome of the informal procedure. This period is necessary to evaluate the policy, reply to legal questions and identify possible recurrent cases.* *If at the date of the expiration of the initial five years, there are ongoing legal or administrative proceedings, which may necessitate the consultation of the files, records shall be kept until the rights for appeal expire.* *The Confidential Counsellor does not keep any personal data beyond the time limit necessary for him or her to accomplish his /her task.* *The Confidential Counsellor shall not keep data more than three months after having finished his/her tasks and closure of the case (file closing form). When the term expires, the documents sent by the alleged victim are returned to him or her or handed in to the Anti-Harassment Coordinator with the alleged victim's explicit consent in line with the security measures described below.* *If the alleged harasser has not been informed of the existence of an informal procedure, no data relating to him/her shall be kept in the archives of the Anti-Harassment Coordinator.* b) Storage period: EACEA applies the principles and retention periods indicated in Common Retention List of the Commission[2] by analogy. The storage periods are the same as indicated for the retention period in point 1.10. c) Is any further processing for historical, statistical or scientific purposes envisaged, which would go beyond the normal retention period? **Yes:** At the end of each year, anonymous statistical data are collected and analysed to enable an assessment to be made of developments in the situation and, where appropriate, to adapt the action to be taken, notably as regards prevention. Confidential Counsellors are responsible for completing an anonymous statistical form for each case handled, even if only in a brief and informal manner. The file opening and closing forms are sent to the Anti-Harassment Coordinator of the Agency where the victim works once a case has been closed.
11	**Recipients of the data**
	Data will only be transmitted to the competent bodies (below mentioned as recipients) when the procedure is launched and with the prior explicit consent of the person who gave them to the recipients. Transmission without explicit prior consent can only occur in exceptional cases covered by Article 5.1 (e) of the Regulation, i.e. when necessary to ensure the protection of the alleged victims (vital interest).

[1] SEC (2019) 900/2 - ARES(2019)4374520 – 09/07/2019
[2] SEC (2019) 900/2 - ARES(2019)4374520 – 09/07/2019

	Recipients: - Confidential Counsellors; - Anti-Harassment Coordinator; - Director, Heads of Department; - Departments of the Agency or services of EU Institutions and bodies (Medical Service, Legal Service, Security Directorate, DG HR,); - In case of audits or proceedings, etc., EACEA's Internal Controller, Legal Sector, DPO In addition, data may be disclosed to public authorities, which are not regarded as recipient in accordance with Union and Member State law. The processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purpose of the processing: • The European Court of Justice or a national judge as well as the lawyers and the agents of the parties in case of a legal procedure; • The competent Appointing Authority in case of a request or a complaint lodged under Articles 90 of the Staff Regulations; • OLAF in case of an investigation conducted in application of Regulation (EC) No 1073/1999; • The Internal Audit Service of the Commission within the scope of the tasks entrusted by article 118 of the Financial Regulation and by article 49 of the Regulation (EC) No 1653/2004; • HR IDOC in line with Commission Decision of 12 June 2019 laying down general implementing provisions on the conduct of administrative inquiries and disciplinary proceedings - C(2019)4231 and Commission Decision (EU) 2019/165 of 1 February 2019 Internal rules concerning the provision of information to data subjects and the restriction of certain of their data protections rights in the context of administrative inquiries, pre-disciplinary, disciplinary and suspension proceedings; • The Court of Auditors within the tasks entrusted to it by Article 287 of the Treaty on the Functioning of the European Union of the EC Treaty and Article 20, paragraph 5 of Regulation (EC) No 58/2003; • The European Ombudsman within the scope of the tasks entrusted to it by Article 228 of the Treaty on the Functioning of the European Union; • The European Data Protection supervisor in accordance with Article 58 of the Regulation. • The European Public Prosecutor's Office within the scope of Article 4 of Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office
12	**Are there any transfers of personal data to third countries or international organisations? If so, to which ones and with which safeguards?**
	Not applicable
13	**<u>General</u> 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. **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. To guarantee security of confidential data provided to Confidential Counsellors and the Head of Anti-Harassment Coordinator (or the Head of Human Resources Service) respectively, all written exchanges must be in paper-copy in envelopes marked as 'Private and confidential'. All transfer of documents other than to the recipient is forbidden. All notes taken during meetings and other documents compiled in a given case are kept in a locked cabinet or drawer (recommended safe boxes whenever possible). This concern the time when the documents are held by the Confidential Counsellor as well as when all documents have been sent to the Anti-Harassment Coordinator. Where documents are stored on an electronic medium, data shall be protected by password or kept on an secured drive, to prevent unauthorized access of third parties. Transfer of documents between the Confidential Counsellor and the Anti-Harassment Coordinator, especially the closing form and files of a case must be delivered by hand in an envelope marked "staff matters and confidential". For the purposes of policy monitoring, and to avoid single cases being recorded twice, the Anti-Harassment Coordinator allocates files a unique number (comprising digits and letters), which it will forward to the Confidential Counsellor responsible for a case. From this point onwards, with a view to preserving confidentiality, the files will be identified solely by their numerical codes and no names will be included in file references. Recipients of data transfer are reminded of their obligation of confidentiality & to use the personal data only for the purposes for which they have been transmitted and that the principle of confidentiality applies to all personal data. In addition, a Code of Ethics of Confidential Counsellors and persons seeking assistance was adopted. **Technical measures:** All communication between the anti-harassment coordinator and the Confidential Counsellor shall be made through an anonymised number code. All written exchanges must be made in envelopes marked as "private and confidential." Data may also be kept in an secured drive by the Confidential Counsellors and the Anti-Harassment Coordinator. The use of encrypted messages (i.e. SECEM) shall also apply. State of the art technical cybersecurity measures are implemented in the corporate systems, according to the security needs. Those measures are in constant evolution.
14	**Information to data subjects / Privacy Statement**
	A Privacy Statement relevant to this data processing activity is available on the EACEA Intranet.