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 *05//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.*

Administrative Inquiries and Disciplinary Proceedings	
1	**Last update of this record (where applicable)**
	22/10/2021
2	**Short description of the processing**
	The Human Resources sector (hereinafter referred to as "EACEA HR") of the EACEA defines, coordinates and ensures implementation of human resources policies (covering the implementation of the procedures for general administrative inquiries and disciplinary issues) within the Agency, on the basis of the relevant provisions of the Staff Regulations (Council Regulation (EEC, Euratom, ECSC) No 259/68 of 29 February 1968 laying down the Staff Regulations of Officials of the European Communities (the "Staff Regulations") and the Conditions of Employment of Other Servants of the European Union.

	The processing of personal data in the framework of general administrative inquiries and disciplinary proceedings is based on a task to be performed in the public interest as provided for in the Staff Regulations and is considered as necessary to comply with the Staff Regulations.
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, BE-1049 Brussels The person designated as being in charge of the processing operation is the Head of Unit of R1 (People, Workplace and Communication) of the EACEA. Email: EACEA-HR@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)**
	EACEA has assigned to the Investigation and Disciplinary Office of the European Commission (IDOC) the role of “full case handling service” including the stages of administrative inquiries and disciplinary procedures. The powers of the Authority Enabled to Conclude Contract of Employment (AECC) remain with EACEA, with IDOC carrying out the ‘operational’ part of the procedure.
7	**Purpose of the processing**
	The data processing aims at allowing the AECC and IDOC, on behalf of the Agency, to evaluate on the basis of information gathered via inquiries if there was a breach by a staff member of his or her obligations under the Staff Regulations and, if necessary, to issue a disciplinary penalty. EACEA and IDOC control and process personal data to fulfil this mission (Service Level agreement between the Agency and DG HR signed on 15 December 2017 (ref. Ares(2017)6169601) including the services provided by Directorate HR.IDOC as set out in Appendix IDOC of the SLA). Preliminary assessment: when the Agency is informed of a situation with a possible disciplinary dimension, it forwards the available information to IDOC for assessment. At the end of the preliminary assessment, IDOC issues a recommendation to the AECC: not to follow-up a case (to treat it as a "non-case"), to refer the case to OLAF, to open an administrative inquiry, or to organise a preliminary hearing (Article 3 of Annex IX of the Staff Regulations, 'pre-disciplinary' stage) directly. IDOC conducts administrative inquiries, pre-disciplinary, disciplinary and suspension proceedings on behalf of the Agency (based on a specific mandate). It also takes part in inquiries carried out to assess whether the professional environment of staff member(s) contributed to an occupational disease. IDOC collects and processes personal data in the context of its proceedings.
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: this includes staff members and former staff members: officials in active employment, on secondment, on leave on personal grounds, on non-active status, on leave for military service, on parental or family leave; officials on disability and retired officials; temporary staff and former temporary staff; contract staff and former contract staff; national experts; trainees and persons employed under private law contracts working on Agency premises.
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: **identification and administrative data of the staff member(s) concerned** ☒ concerning the physical characteristics of persons as well as the image, voice or fingerprints ☐ concerning the data subject's private sphere: external activities, friends, hobbies, sports, etc.; ☒ concerning pay, allowances and bank accounts ☒ concerning recruitment and contracts: category of staff, grade, step, duration of the contract, documents relating to the work of the selection committee; ☒ 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**:

- Data concerning allegations / declarations
- Data relating to personal details of the data subject: surname at birth, current surname, forename, street, postcode, place, country, date of birth, town/city of birth, country of birth, sex, nationality, other nationality, telephone numbers, e-mail address, ISDN number, social media relating to the investigation and disciplinary action;
- Data relating to behaviour, action or inaction of the person(s) subject to an administrative inquiry and/or a disciplinary proceeding;
- Data relating to legal qualification of that behaviour, action or inaction having regard to the Staff Regulations and other obligations incumbent on the person concerned;
- Data relating to individual responsibility of the person(s) concerned, including financial liability (Article 22 of the Staff Regulations which applies by analogy to the EACEA staff);
- Data relating to disciplinary measures taken against the person concerned where appropriate;
- Data relating to suspected offences, committed offences, criminal convictions or security measures;
- Data related to hearings via the written procedure (i.e. whenever the data subject concerned cannot be heard under the provisions of Annex IX of the Staff Regulations);
- Data relating to the legal representative or accompanying person of the data subject: name, surname, address;
- Data relating to witnesses: name, address, telephone numbers, email address;
- Data relating to any persons affected or harmed by the data subject (name, surname, medical data, details of behaviour or actions) leading to the disciplinary procedure;
- Traffic data: Personal data relating to internet connections and/or the use of email or telephone may be processed (for example by IDOC) in the course of an administrative inquiry and/or disciplinary proceedings. In this case, the data minimisation principle (Article 4.1(c) of the Regulation) will be applied and IDOC processes only appropriate, relevant and not excessive traffic data in relation to the purpose for which they are further processed (investigation purpose).
- When IDOC, or where applicable the AECC consider it appropriate, the hearing may also be audio recorded or held via videoconference (IDOC Guide and Commission Decision C(2019)4231 final which has been adopted by analogy by the EACEA in its decision Ref. Ares(2019)6296355 of 11/10/2019).
- Electronic communications
  In case the AECC considers it necessary to process data that relate to Internet connections, the e-mail or the telephone use within the context of an administrative inquiry or disciplinary proceeding, it will do so with due observance of the provisions of the Article 25 of the Regulation implemented by Decision of the Steering Committee on internal rules concerning restrictions of certain rights of data subjects in relation to the processing of personal data in the framework of activities carried out by the Education, Audiovisual and Culture Executive Agency and published in the Official Journal of the European Union (OJ L92, 17/03/2021).

It may be possible that other personal data needs to be processed but cannot be identified at the stage of the prior check, depending on the nature of the case being dealt with.

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:*** depending on the reason or action forming the basis of the investigation and disciplinary action, EACEA may need to process special categories of personal data.
10	**Retention time (time limit for keeping the personal data)**
	The Agency applies the principles and retention periods indicated in the Common-Level Retention List for European Commission Files by analogy (the updated version of the list can be found on the EACEA Intranet) **Administrative investigations** Files containing documents for which a decision has been taken not to launch an administrative investigation are retained for a period of 5 years before being destroyed. **Investigations with disciplinary consequences** Files containing the investigation report, instruments of the disciplinary procedure, correspondence with the person(s) concerned, the decision imposing disciplinary measures and any follow-up (appeals) are retained for a period of 15 years before being transferred to the historical archives for permanent preservation. **Investigations without disciplinary consequences** Files containing the investigation report and the documents for which the decision was taken to open a disciplinary procedure are retained for a period of 15 years before being destroyed or transferred to the historical archives for permanent preservation if the lead department is OLAF. **Disciplinary procedures** Files containing documents for which the decision was taken to open a disciplinary procedure, including the instruments of the disciplinary procedure, correspondence with the person(s) concerned, the decision imposing disciplinary measures and any follow-up (appeals) are retained for a period of 20 years before being destroyed. **Cooperation in investigations and disciplinary procedures** Files created by the Agency cooperating with HR and OLAF during these investigations and disciplinary procedures are retained for a period of 15 years by the SG and 5 years by the Agency before being destroyed. Files covering complaints to the administration under Article 90(2) of the Staff Regulations and requests for assistance under Article 24 and 90(1), as well as complaints or requests under Article 22(c) are retained for a period of 15 years before being transferred to the historical archive for permanent preservation. IDOC may require the Agency to process personal data/traffic data relating to internet connections and/or the use of e-mail or telephone in the course of an administrative inquiry and/or disciplinary proceedings., This personal data will be erased by the Agency once the file has been transmitted to IDOC, IDOC may keep the file for a longer period to establish, exercise or defend a right in a legal claim pending before a Court, OLAF and/or the European Ombudsman.

	Personal files • In accordance with Article 22(2) of Annex IX of the Staff Regulations, if the AECC decides to close the case without imposing any disciplinary penalty, and it informs the person concerned accordingly in writing without delay, there shall be no record of this decision in the personal file unless upon request of the person concerned. • Concerning the retention of the disciplinary decision that imposes a penalty/sanction on the staff member concerned, a copy of the decision will be kept in the personal file of the jobholder according to Article 27 of Annex IX of the Staff Regulations that determines the time limits from when the person concerned may request the withdrawal of any mention of the disciplinary measure that figures in the disciplinary file: i. 3 years in case of a written warning or reprimand ii. 6 years in case of any other penalty. The AECC shall decide whether to grant this request. • Personal data will be kept beyond the time-limits indicated above where they may be required for consultation in the context of legal or administrative procedures (for example claims for damages, requests by the Ombudsman, appeals to the Court of Justice etc.) which are still pending when the time-limit expires. **Is any further processing for historical, statistical or scientific purposes envisaged?** ☐ yes ☒ no
11	**Recipients of the data**
	Data may be disclosed to the following recipients on a need-to-know basis (the type of recipient may vary according to the type of administrative inquiries and during disciplinary proceedings): Within the Agency: • Director of the Agency in his/her capacity of AECC; • Heads of Department; • Head of Unit R1; • Head of HR Sector; • EACEA HR Sector (HR staff in charge of the file); • EACEA Internal services (Legal Service, Internal Control) • Head of Unit R2; Outside the Agency: • DG Human Resources and Security (DG HR); • Investigations and Disciplinary Office (IDOC); • Office for the Administration and Payment of individual Entitlements (PMO); • Medical Service; • Doctor(s) appointed by the Agency; • Doctor(s) appointed by the data subject concerned; • Medical Committee; • European Anti-Fraud Office (OLAF); • European Data Protection Supervisor (EDPS); • Financial Irregularities Panel (PIF); • European Court of Auditors (ECA); • European Ombudsman; • The Court of Justice of the European Union (Court of Justice, the General Court of the European Union); • Competent authorities of the Member States. Transfers to competent national

	authorities such as a National Court may occur where there is an infringement of national law and if such a transfer is necessary for the performance of a task carried out in the public interest or subject to the exercise of public authority of the national authorities. • Financial Irregularities Panel: where the facts identified lead to a suspicion of financial irregularities, the conclusions related to the facts are communicated to the specialised Financial Irregularities Panel (Articles 66(8) and 73(6) of the Financial Regulation). • EACEA Disciplinary Board (depending on the constitution of the Board, this will comprise of current staff of EACEA and staff/seconded officials from other Agencies who are appointed to the Board. It will also include any former staff members on the Board in the role of Chair/Vice-Chair) Any recipient of the data shall be reminded of their obligation not to use the data received for other purposes than the one for which they were transmitted.
12	**Are there any transfers of personal data to third countries or international organisations? If so, to which ones and with which safeguards?** N/A
13	**General description of the technical and organisational security measures** Organisational measures Organisational measures include appropriate access rights and access control precautions. More specific, access to the data (ARES, functional mailboxes, paper files, shared folders on the EACEA file server, etc.) is granted only to authorised members of the EACEA staff on a need to know basis. Relevant communication by email will be sent encrypted by using SECEM. The authentication for HERMES-ARES-NOMCOM (HAN) is performed via the European Commission Authentication Service (ECAS) mechanism, which is designed to increase the security of the European Commission IT systems. Technical measures Technical measures include the use of secure equipment (e.g. locked cupboards and safes) and IT tools (including file servers, email servers, secure connections, firewalls, etc.). All data in electronic format (data, emails, etc.) that is collected and processed during this processing operation are stored either on the servers of the European Commission or of the EACEA, the operations of which abide by the European Commission's security decisions and provisions established by the Directorate of Security for this kind of servers and services. The paper files will be stored in a cupboard (locked) located in the EACEA HR archive room (locked). Access will be granted only to authorised agents staff of the Agency on a need to know basis. Advanced Records System (ARES) The HERMES – ARES – NOMCOM (HAN) is an IT system of the European Commission. ARES is a document management system, linked to "HERMES", used by the European Commission and Executive Agencies. ARES is hosted on secure servers of the Commission. Electronic documents containing personal data will be transferred and archived via ARES, which provides security for sensitive documents in two simultaneous ways: the marking and the filing. Marking in ARES There is a special marking that will be applied when we will process personal data in the context of administrative inquiry and disciplinary investigations, which is called

	"Investigations and disciplinary matters". Attachments can be done in ARES. Filing In order to ensure limited access to a file, a predefined group of users identified by the controller will be created. The file will only be visible to the predefined group identified by the controller on a need to know basis. Only people having received both the right to read the marking and to have access to the file will be allowed to consult the documents. The audit trails for data processing and communication will be done via ARES workflow. Considering the use of ARES for each transmission and storage of personal data according to the above mentioned measures, no undue removal or undue transmission will be possible.
14	**Information to data subjects / Privacy Statement**
	Privacy Statements relevant to these data processing activities are available on the EACEA Intranet.