



European Research Council
Executive Agency

Established by the European Commission

RECORD OF PERSONAL DATA PROCESSING

Art. 31 of the 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 "Data Protection Regulation")

Record n°

DPO 56 -2021

In accordance with Article 31 of the data protection regulation, individuals whose personal data are processed by the Executive Agency in any context whatsoever are to be protected with regard to the processing of personal data and the Executive Agency has to keep records of their processing operations.

This record covers two aspects:

1. Mandatory records under Art 31 of the data protection 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 if applicable	Ares(2014)4275854 – 18/12/2014
2	Short description of the processing	As soon as the Agency is informed of or identifies a situation with a possible disciplinary dimension, it forwards the available information to HR.IDOC for its assessment. IDOC conducts administrative inquiries, pre-disciplinary, disciplinary and suspension proceedings on behalf of the Agency. 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.

Part 1 - Article 31 Record

3	Function and contact details of the controller	Head of the Human Resources Unit (ERCEA.D.2) ERC-HR-COMPLAINTS@ec.europa.eu
4	Contact details of the Data Protection Officer (DPO)	ERC-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)	Investigation and Disciplinary Office of the European Commission (HR.IDOC) HR-MAIL-IDOC@ec.europa.eu Directorate-General for Informatics (DG DIGIT) DIGIT-SYSPEP2@ec.europa.eu External service providers for the deployment of communication services.
7	Purpose of the processing	The data processing aims at allowing the Authority Empowered to Conclude Contracts (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. The Agency informs IDOC of a situation with a possible disciplinary dimension by forwarding all the available information (including those collected during the pre-inquiry) to HR.IDOC for assessment (see SLA with HR.IDOC). IDOC conducts administrative inquiries, pre-disciplinary, disciplinary and suspension proceedings on behalf of the Agency. 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. The Agency reserves its right to contact the staff member via his/her private phone number and e-mail address when deemed necessary with the sole purpose of ensuring the effective application of the relevant provisions of the SR and the CEOS. The Controller may envisage anonymous statistical analyses with the purpose of improving the quality of the processes.

8	Description of the categories of data subjects	☒ EA staff including former staff [Temporary Staff, Contract Staff]. ☐ Visitors to the EA ☒ Contractors providing goods or services [Intra-muros experts, interim staff, persons employed under private law contracts working on the Agency's premises]. ☐ Applicants ☐ Relatives of the data subject ☐ Complainants, correspondents and enquirers ☒ Witnesses ☐ Beneficiaries ☒ External experts [Seconded National Experts]. ☒ Other: [Blue Book trainees]. [The person under investigation, third parties (indicated in the file) and alleged victims (if any)]. [Legal representative or accompanying person of the data subject]
9	Description of personal data categories Indicate all the categories of personal data processed and specify which personal data are being processed for each category (between brackets under/next to each category):	<i>Categories of personal data:</i> ☒ in the form of personal identification numbers [E.g. personnel number, ISDN number]. ☒ concerning the physical characteristics of persons as well as the image, voice or fingerprints [Image, video, voice]. ☒ concerning the data subject's private sphere [E.g. external activities, hobbies, sports]. ☒ concerning recruitment and contracts and the data subject's career [Category of staff, grade, step, duration of the contract, documents relating to the work of the selection committee Organisation (Sector, Unit, Department)]. [Information on salary, allowances and bank accounts] ☒ concerning the data subject's family

	☐ concerning leave and absences ☒ concerning missions and journeys ☒ concerning social security and pensions ☒ concerning expenses and medical benefits ☒ concerning telephone numbers and communications [Phone number, office number]. ☒ concerning names and addresses (including email addresses) [Name, surname, private and professional address and e-mail address]. ☒ Other: [Date and place of birth, gender, nationality]. <i>Categories of personal data processing likely to present specific risks:</i> ☒ data relating to suspected offences, offences, criminal convictions or security measures [Data relating to individual responsibility of the person(s) concerned, including financial liability (Art. 22 of the SR which applies by analogy to the ERCEA 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 SR)]. ☒ data being used to evaluate personal aspects of the data subject (ability, efficiency, conduct) [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 SR and other obligations incumbent on the person concerned]. Categories of personal data whose processing is <u>prohibited</u>, with exceptions (art. 10 new Regulation): ☐ 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 Depending on the reason or action forming the basis of the investigation and disciplinary action, the ERCEA may need to process special categories of personal data. For example:: racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. <i>Specify any additional data or explanatory information on the data being processed, if any:</i> Social media relating to the investigation and disciplinary action. 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). Data concerning allegations / declarations
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, as detailed below: 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 DG/Agency before being destroyed. Files covering complaints to the administration under Article 90(2) of the SR 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. <u>Personal files</u> • In accordance with Article 22(2) of Annex IX of the SR, 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 SR 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: 3 years in case of a written warning or reprimand 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 archiving purposes in the public interest, historical, statistical or scientific purposes envisaged? ☒ yes ☐ no
--	---

		The ERCEA may envisage anonymous statistical analyses with the purpose to improve the quality of the processes and the management of human resources.
11	Recipients of the data	Personal 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): <u>Within the Agency:</u> • The Authority Empowered to Conclude Contracts (AECC), i.e., the ERCEA's Director and Heads of Department; • The members of the HR Unit and authorised personnel dealing with administrative inquiries and disciplinary proceedings;; • The Legal Affairs and Internal Control Unit; <u>Outside the Agency:</u> • 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). The Disciplinary Board; depending on the constitution of the Board, this will comprise of current staff of ERCEA 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	All personal data in electronic format (e-mails, documents, databases, uploaded batches of data, etc.) that are processed during this processing activity are stored either on the servers of the European Commission or of the ERCEA, the operations of which abide by the European Commission's security decisions and provisions established by the Security Directorate and DG DIGIT for such servers and services. In order to protect personal data, the ERCEA has put in place a number of technical and organisational measures. Technical measures include appropriate actions to address online security, risk of data loss/theft/breach, alteration of data or unauthorised access, taking into consideration the risk presented by the processing and the nature of the personal data being processed. Organisational measures include restricting access to the personal data solely to authorised persons with a legitimate need to know for the purposes of this processing operation. The data collected and the documents created by the ERCEA, which contain personal data are stored in the case file, which is encrypted. These files can only be accessed by authorised staff with the necessary access rights. All hard copy data are kept securely in the ERCEA premises and can only be accessed by authorised staff with the necessary access rights. ERCEA staff members apply strict measures to ensure that the personal data are not accessed by unauthorised persons. This includes the use of locked cabinets, encrypted email and printing via presentation of personnel badges. Relevant electronic communications should be sent via SECEN-encrypted email. Access to data is granted only to authorised staff members of the ERCEA.

14	Information to data subjects/Data Protection Notice (DPN)	The Data Protection Notice is available on the Intranet page of the Agency: http://intranet.ercea.cec.eu.int/services/human-resources/priv/Pages/default.aspx
----	--	---