



## EUROPEAN COMMISSION

European Climate, Infrastructure and Environment Executive Agency (CINEA)

**RECORD OF PERSONAL DATA PROCESSING ACTIVITY**

In accordance with Article 31 of the [Data Protection Regulation for EUIs](#)<sup>1</sup> (hereinafter referred to as the Regulation), individuals whose personal data are processed by the Innovation and Networks Executive Agency (hereinafter referred to as CINEA 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: 2021-1/R4-HR-16  
Created on (date): 27/1/21  
Last update (date): 25/08/21

**NAME OF THE PROCESSING ACTIVITY**

Administrative Inquiries and Disciplinary Proceedings

**GROUND FOR THE RECORD :**

- Regularisation of a data processing activity already carried out  
This record replaces notification n° HR-25 issued under the previous Data Protection Regulation. This is a migration from notification to record
- Record of a new data processing activity prior to its implementation
- Change of a data processing activity (e.g.: update of a record).

<sup>1</sup> Regulation (EU) 2018/1725 of 23 October 2018

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

### 1.1. Name and contact details of controller

- a. CINEA.A4  
Chaussée de Wavre 910  
W910 03/004  
BE – 1049 Brussels
- b. the Head of Unit CINEA.A4
- c. Email: [CINEA-HR-Staff-Administration@ec.europa.eu](mailto:CINEA-HR-Staff-Administration@ec.europa.eu)

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

Agency DPO - [CINEA-DPO@ec.europa.eu](mailto:CINEA-DPO@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)

The Agency 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 the Agency and IDOC is carrying out the ‘operational’ part of the procedure.

Email: DG HR IDOC: [HR-MAIL-IDOC@ec.europa.eu](mailto:HR-MAIL-IDOC@ec.europa.eu)

This is based on the Service level Agreement (SLA) between the Agency and DG HR (Ares(2018)102092) signed on 22/12/2017

### 1.5. 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. The Agency (EA) as AECC and IDOC process personal data to fulfil this mission.

When the EA is informed of a situation with a possible disciplinary impact, it forwards the available information to HR.IDOC for an assessment. HR IDOC may also be informed of a situation with a possible disciplinary impact via other sources.

IDOC carries out preliminary assessments, administrative inquiries, pre-disciplinary and disciplinary proceedings. It may conduct suspension proceedings on behalf of the Appointing Authority.

IDOC also takes part in inquiries carried out by DG HR to assess whether the professional environment of a staff member contributed to an occupational disease<sup>2</sup>.

IDOC collects and processes personal data in the context of its proceedings.

#### 1.6. Legal basis for the processing

The processing is necessary for the performance of tasks carried out in the public interest or in the exercise of official authority vested in the Union institution or body (Article 5(1)(a) of the Regulation) and for compliance with a legal obligation to which the controller is subject (Article 5(1)(b) of the Regulation), as established by the following legal acts:

- 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 ;
- Commission Implementing Decision (EU) 2021/173 of 12 February 2021 establishing the European Climate, Infrastructure and Environment Executive Agency, and repealing Implementing Decisions 2013/801/EU ;
- Commission Decision C(2021)947 of 12 February 2021 delegating powers to the European Climate, Infrastructure and Environment Executive Agency with a view to the performance of tasks linked to the implementation of Union programmes in the field of transport and energy infrastructure; climate, energy and mobility research and innovation; environment, nature and biodiversity; transition to low-carbon technologies; and maritime and fisheries;
- Articles 22, 73 and 86 and Annex IX 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 and articles 49, 50 and 119 of the Conditions of Employment of Other Servants of the European Communities (the "CEOS");
- Commission Decision C(2019) 4231 of 12/06/2019 laying down general implementing provisions on the conduct of administrative inquiries and disciplinary procedures which has been adopted by analogy by the CINEA Steering Committee in its decision SC(2019)023 of 20/09/2019;

The Agency may process special categories of personal data under Articles 10(2) of the Regulation in cases where:

- the processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law insofar as it is authorised by Union law providing for appropriate safeguards for the fundamental rights and the interests of the data subject 10(2)(b);
- the processing relates to personal data which are manifestly made public by the data subject (Article 10(2)(e)).
- the processing is necessary for the establishment, exercise or defence of legal claims or whenever the Court of Justice is acting in its judicial capacity (Article 10(2)(f)).
- the processing is necessary for reasons of substantial public interest, on the basis of Union law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to

---

<sup>2</sup> See Article 16 of the Common rules on the insurance against the risk of accident and of occupational disease and Administrative Notice N° 15-2018 of 4 April 2018.

safeguard the fundamental rights and the interests of the data subject (Article 10(2)(g)).

### 1.7. Categories of data subjects

Statutory staff (Contract Agents, Temporary Agents, Seconded Officials)<sup>3</sup>, national experts, trainees and persons employed under private law contracts working on Agency premises. It includes the person under investigation, - if applicable - his/her representative, witnesses, third parties (i.e. relevant persons indicated in the file such as witnesses, etc.) and alleged victims (if any).

### 1.8. Categories of personal data

In the course of its proceedings, the Agency and IDOC receive and collect personal data.

At the outset of a case, the Agency and IDOC process initial information that usually contains personal data about the person subject of the allegations.

For the person(s) connected to the allegations, either because they are the target of these allegations or because they could bring information in this respect, IDOC may collect data regarding the identity, duties, contact details, information concerning the career, skills, knowledge of languages, training, professional experience and any other data relevant to the data processing operation in question. The data may also include information relating to their behaviour or their perception of the facts of the case. The data processed by IDOC is subject to a specific record and data protection notice.

#### List of data categories:

- Identification and administrative data;
- Case-related data (allegations / declarations etc.);
- Special categories of personal data (dependent upon the nature of the case);
- 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, gender, nationality(ies), telephone numbers, e-mail address, ISDN number (mobile & data communication), social media relating to the investigation and disciplinary action;
- Data relating to behavior, action or inaction of the person(s) subject to an administrative inquiry and/or a disciplinary proceeding;
- Data relating to legal qualification of that behavior, action or inaction having regard to the SR and other obligations incumbent on the person concerned;
- Data relating to individual responsibility of the person(s) concerned, including financial liability (Art. 22 of the Staff Regulations which applies by analogy to the staff of the Agency);
- Data relating to disciplinary measures taken against the person concerned where appropriate;
- Data relating to suspected offences, committed offences, criminal convictions or security measures;

---

<sup>3</sup> 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

- 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 behavior or actions) leading to the disciplinary procedure;
- Data in the form of personal identification numbers (personnel number, department, unit, sector);
- Data relating to the physical characteristics of the data subject (i.e. image/video);
- Data concerning the private life of the data subject (external activities, relationship, hobbies, sports, etc.);
- Data concerning salary, allowances and bank accounts of data subject;
- Data concerning recruitment and employment contracts of data subject (category of staff, grade, step, duration of the contract, documents relating to the work of the selection committee);
- Data concerning the data subject's family;
- Data concerning missions and journeys of the data subject;
- Data concerning social security and pensions of the data subject;
- Data concerning expenses and medical benefits of the data subject;
- 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 minimization principle (Article 4.1(c) of the Regulation) will be applied and IDOC will process 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).
- Electronic communications; In case the AECC considers it necessary, data that relate to Internet connections, the use of e-mail or telephone within the context of an administrative inquiry or disciplinary proceeding may be processed: it will do so with due observance of the provisions of the Article 25 of the Regulation.

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

#### **a) Retention period:**

The Agency applies the principles and retention periods indicated in the Common-Level Retention List for European Commission Files by analogy, as detailed here below, see: [https://ec.europa.eu/info/sites/info/files/sec-2019-900\\_en.pdf](https://ec.europa.eu/info/sites/info/files/sec-2019-900_en.pdf)<sup>4</sup> :

#### **Administrative investigations**

---

<sup>4</sup> SEC (2019) 900/2 - ARES(2019)4374520 – 09/07/2019

Files containing documents for which a decision was 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 SG and 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 HR(IDOC)/Agency before being destroyed.

Files covering complaints to the administration under Article 90(2) and requests for assistance under Article 24 and 90(1) of the Staff Regulations, as well as complaints or requests under its 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.

b) Storage period:

The storage periods are the same as indicated for the retention period in point 1.9 a).

c) Is any further processing for historical, statistical or scientific purposes envisaged, which would go beyond the normal retention period? **No**

#### 1.10. 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:**

Data may be disclosed to recipients such as for instance:

- Authority Empowered to Conclude Contracts (AECC) within the Agency;
- Heads of Department;
- Head of Unit HR, IT and Logistics
- Head of Sector HR;
- HR Sector (HR staff in charge of the file);
- Relevant internal services (e.g.: Legal Sector, Internal Control, DPO, etc)
- The Agency's Disciplinary Board; (depending on the constitution of the Board, this will comprise of current staff of the Agency 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).

##### **Outside the Agency:**

During the closure of an inquiry, pre-disciplinary or disciplinary proceedings, personal data relating to administrative inquiries & disciplinary proceedings can be communicated to other services on a need-to-know basis only. This is done, for example, because of their role in processing or following up on the disciplinary file. The information may be communicated, upon request, to services such as for instance:

- Investigations and Disciplinary Office (IDOC);
- European Anti-Fraud Office (OLAF);
- DG Human Resources and Security (DG HR);
- Secretariat-General (SG);
- Legal Service;
- 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 Data Protection Supervisor (EDPS);
- Financial Irregularities Panel (PIF): 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);
- 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;
- The competent Appointing Authority in case of a request or a complaint lodged under Articles 90 of the Staff Regulations;
- 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;
- 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.

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.

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

Not applicable

#### **1.12. Description of 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 Agency, 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 Agency 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 Agency which contain the 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 premises of the Agency and can only be accessed by authorised staff with the necessary access rights.



The staff of the Agency 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 are sent via SECEM encrypted email.

Access to data is granted only to authorised members of the Agency staff which is authorised by the Head of Unit of the Human Resources Sector on a case-by-case basis.

Confidentiality of communications:

- The AECC is aware of the obligation to ensure confidentiality of electronic communications (telecommunications networks and terminal equipment) as provided for in Articles 36 and 37 of the Regulation.
- If the AECC considers that it is necessary to gain access to electronic communications in the course of an administrative inquiry or disciplinary proceeding (and only on a case by case basis), the criteria defined in the respective EDPS guidelines and in the Regulation, namely, inter alia lawfulness, necessity, proportionality and choice of the less intrusive means of investigation will be observed.
- It may be possible that the Agency (including IDOC for administrative inquiries under Annex IX of the Staff Regulations and disciplinary proceedings before the Agency's Disciplinary Board) needs to process data that cannot be identified at the stage of the preparation of this record and that can vary according to the nature of the case being dealt with. The Agency (including IDOC for administrative inquiries under Annex IX of the Staff Regulations and disciplinary proceedings before the Agency Disciplinary Board) ensures that data processed are adequate, relevant and limited to what is necessary processed in conformity with Article 4(1)(c) of the Regulation.
- Certain special categories of data as defined Article 10(1) of the Regulation might be processed by the Agency if any exception provided in Article 10(2) or Article 11 of the Regulation applies (including IDOC for administrative inquiries under Annex IX of the Staff Regulations and disciplinary proceedings before the Agency Disciplinary Board). The data processed will ultimately depend on the nature and severity of the disciplinary investigation whilst applying the data minimisation principle.

### **1.13. Data Protection Notice**

A Data Protection Notice (DPN) relevant to this data processing activity is available on the Agency Intranet <https://cineanet.cinea.cec.eu.int/services/human-resources/legal-issues/data-protection>