Ares(2020)5806150 -23/10/2020

EUROPEAN COMMISSION

Innovation and Networks Executive Agency

RECORD OF PERSONAL DATA PROCESSING ACTIVITY

In accordance with Article 31 of the Data Protection Regulation for EUIs[1] (hereinafter referred to as the Regulation), individuals whose personal data are processed by the Innovation and Networks Executive Agency (hereinafter referred to as INEA 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: 2020-29/R4-HR-15b
Created on (date): 07.07.20
Last update (date): 22.10.20 N° de sauvegarde: inea.r.r04.r41(2020)6499687

NAME OF THE PROCESSING ACTIVITY

Processing of personal data within the framework of the anti-harassment policy

GROUND FOR THE RECORD :

☒ *Regularisation of a data processing activity already carried out*
This record replaces notification n° HR-23 & 24 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).*

[1] 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. INEA

Chaussée de Wavre 910

W910 04/136

BE – 1049 Brussels

b. the Head of Unit R.4

c. Email: INEA-Harassment@ec.europa.eu

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

INEA DPO

INEA-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)

Not applicable

1.5. 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.

1.6. Legal basis for the processing

- Council Regulation (EC) No 58/2003 of 19 December 2002 laying down the statute for executive agencies to been trusted with certain tasks in the management of Community programmes;
- Commission Decision 2013/801/EU of 23 December 2013 establishing the Innovation and Networks Executive Agency and repealing Decision 2007/60/EC as amended by Decision 2008/593/EC;
- Commission Decision C(2013)9235 of 23 December 2013 delegating powers to INEA with a view to the performance of tasks linked to implementation of the Union programmes in the field of transport, energy, telecommunications infrastructure and in the field of transport and energy research and innovation, comprising in particular implementation of appropriations entered in the general budget of the Union;
- Staff Regulations on officials of the European Communities and the Conditions of employment of other servants of the European Communities: Articles 1 (d), 12, 12 (a), Article 24 and Articles 11 and 81 of the CEOS. Article 12 (a) of the Staff Regulations provides that "officials shall refrain from any form of psychological harassment";
- Memorandum of Understanding for the setting up of a network of Confidential Counsellors;
- Decision SC (2020) 26 of the INEA Steering Committee of 14 October 2020 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 Innovation and Networks Executive Agency

1.7. Categories of data subjects

Seconded officials, temporary agents, contractual agents, interim staff, people working under national contracts, trainees and project applicants/beneficiaries or experts, visitors etc. , namely any persons potentially concerned, who could be alleged harasser, alleged victim, witness or other person implicated.

1.8. Categories of personal data

- 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. In particular, sensitive data relating to physical or psychological harassment might be processed.

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

[a) Retention period:

The Agency applies the principles and retention periods indicated in Common Retention List of the Commission[2].

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 forwarded 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:

INEA applies the principles and retention periods indicated in Common Retention List of the Commission[3] by analogy. 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 ?

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 form is sent to the Anti-Harassment Coordinator of the Agency where the victim works once a case has been closed.

1.10. 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).

Recipients:

Confidential Counsellors;

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

- 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, etc.);
- In case of audits or proceedings, etc., INEA'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

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

Not applicable

1.12. Description of security measures

Access to data is only possible via restricted access on an individual need to know basis and through User-ID and password. Personal data resides on the servers of the European Commission, which abide by strict security measures implemented by DG DIGIT to protect the security and integrity of the relevant electronic assets.

Organisational measures:

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[4]). 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 encrypted disk, 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 encrypted disk by the Confidential Counsellors and the Anti-Harassment Coordinator. The use of encrypted messages (i.e. SECEM) shall also apply.

1.13. Data Protection Notice

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

[4] INEA uses a safe with a PIN Code. The PIN code was defined and is only known by the anti-harassment coordinator. A copy of the PIN code of the safe is kept for security and back-up purposes in a sealed envelope in the safe of the HR Head of Sector.