



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: 2020-021/R4-HR-18

Created on (date): 11/05/20

Last update (date): 02/09/20 with save n°: [inea.r.r04.r41\(2020\)4452994](#)

NAME OF THE PROCESSING ACTIVITY

Processing of personal data in the context of ethics related procedures

GROUND FOR THE RECORD:

- Regularisation of a data processing activity already carried out
This record replaces notifications HR 30 issued under the previous Data Protection Regulation
- 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. *Head of Unit R.04*
- c. *Email: INEA-HR-INFO@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 Agency collects and uses personal data in the context of authorization requests and various ethical statements in relation to the rights and obligations of statutory staff in order to:

- Examine authorization requests / ethical statements from members and former members of the statutory staff (civil servants, temporary agents, contract agents);*
- To assess whether the requests or declarations present an incompatibility vis-à-vis statutory obligations and / or an incompatibility with the interests of the Institution;*
- To propose to the Appointing Authority to authorize the requests, possibly with restrictions;*
- To propose to the Appointing Authority to refuse (in particular in the event of a real or potential conflict of interest, of incompatibility with the interests of the Institution, etc.);*

Authorisation requests concern for instance:

- *outside activities for staff in active employment;*
- *professional activity during leave on personal grounds;*
- *activities of staff having left the Agency (retirement, end of contract);*
- *permission to receive honours ;*
- *permission to keep a gift;*
- *employment of spouse;*
- *publishing articles and speeches;*
- *participating in electoral campaigns;*
- *exercising an elective public office.*

1.6. Legal basis for the processing

Lawfulness: Article 5 . 1 (a) & (b) of the Regulation:

-processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body;

- processing is necessary for compliance with a legal obligation to which the controller is subject :

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 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;

Articles 11, 11 bis, 12 ter, 13, 15, 16, 17, 17 bis et 40 & Annex VIII (articles 13 and 40)) of the Staff Regulations and corresponding conditions of employment of other servants, (articles 11 et 81)

Commission Decision relating to external activities C (2018) 4048 final of 29 June 2018

Steering Committee Decision SC(2018)020 of 12/10/2018 adopting by analogy of the Commission Decision on outside activities and assignments and on occupational activities after leaving the Service C(2018)4048 of 29 June 2018

Rules governing Ethics in INEA

https://ineanet.inea.cec.eu.int/sites/default/files/sites/default/files/inea_files/Ethics%20guidelines%20final%20-%20jb.pdf

Internal guidelines and recommendations on conflicts of interest management - Ares(2020)2194245 - 23/04/2020

1.7. Categories of data subjects

All statutory staff members of INEA (Temporary and contract agents) and spouses/partners².

1.8. Categories of personal data

The data collected concerning staff members are as follows:

A. Identification Data from Sysper: surname, first name, administrative status, personnel number, sex, NUP, grade and functions, telephone number, address, assignment, job description;

B. Data enabling the appointing authority to take a decision:

² Other staff working for INEA such as persons employed under private law contracts, experts on secondment from national civil services (SNEs), trainees, and external experts follow specific rules regarding their specific employment situation.

1. *Request for authorization for an outside activity during active service: detailed description of the proposed outside activity, nature of the position, calendar, duration, financial link with the Agency, links with the functions exercised at the Agency, type of leave used to cover absence, financial arrangements;*
2. *Request for authorization for an outside activity during leave on personal grounds / after leaving office: detailed description of the proposed outside activity, nature of the post, calendar, duration, financial link with the Agency, links with the functions exercised within the Agency;*
3. *Declaration of employment of the spouse: detailed description of the employment of the spouse, nature of the position, calendar, duration, financial link with the Agency, links with the functions exercised at the Agency;*
4. *Declaration of conflict of interest: description of the nature of the conflict of interest and details of the situation indicating a potential conflict of interest;*
5. *Election to public office: nature of the post, duration, timetable, remuneration, compatibility with the posts at the Agency*
6. *Declaration of publication: title, subject, publisher, date of publication, content of the article whose publication is envisaged;*
7. *Gifts and hospitality offers: description and origin of the gift, estimate of its value, justification; nature and amount of hospitality, context, possible direct or indirect link with the duties of the staff member;*
8. *Opinions and approvals of the different hierarchical levels, decision of the Appointing Authority.*

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

INEA applies the principles and retention periods indicated in Common Retention List of the Commission³ by analogy and PMO specific retention list⁴.

[a) Retention period:

After the closure of authorization requests or miscellaneous ethical statements when these have been the subject of a decision of the Appointing Authority, the data will be retained as follows:

- In the context of authorization requests / declarations in paper version (activity after leaving office,; activity during invalidity; allocation for honors; participation in an electoral campaign; election to public office), the decision of the appointing authority is kept in the staff member's personnel file. This means that the data will be kept as long as the other documents contained in the personal files are kept, namely for at least 100 years after the recruitment of the person concerned and 8 years after the extinction of the rights of the beneficiaries concerned.

- As part of authorization requests / declarations introduced in the module ETHICS of Sysper, the decision of the Appointing Authority is stored in Sysper. The retention period of the decision follows the retention period of the data appearing in Sysper⁵. Certain administrative information linked to the request (for example, the start and end

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

⁴ ARES(2016)6048949 - 21/10/2016

⁵ Information on roles, access rights, organisational entity and activities according to Commission priorities are kept for each assignment during the active career. Logs are kept for 10 years.

dates of leave for personal convenience) stored in Sysper follows the same retention period as the relevant Sysper data.

- All the information necessary for the management of the file (e.g. electronic correspondence with the applicant, traffic sheet) is placed in files (paper) or on a hard disk (HR restricted drive) and is kept for ten years by the Unit R.4.

b) Storage period:

INEA applies the principles and retention periods indicated in Common Retention List of the Commission⁶ 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 The documents may be kept (for example for statistical or documentary purposes) beyond the periods indicated above, but only after the personal data contained in the ethical requests / files have been deleted or made anonymous and for 10 years.*

1.10. Recipients of the data

On a need to know basis:

- *Hierarchical superior of the data subject*
- *HR officers in charge of management of Ethics in the Agency*
- *HR Head of Sector.*
- *The competent Appointing Authority (the Director of the Agency, the delegated Authority and the body in charge of the examination of the request/declaration)*
- *Regarding access to the personal file, to the administrative part of the file, "External activities" tab, the documents therein, namely the decision of the appointing authority, are accessible to the HR team responsible for career management.*

In case of audits or proceedings, etc., INEA's Internal Controller, Legal Team, DPO, Staff Committee, etc

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;*

⁶ SEC (2019) 900/2 - ARES(2019)4374520 – 09/07/2019

- *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 (EC) 2018/1725.*

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

Not applicable

1.12. Description of security measures

Personal data is stored electronically and in paper and accessible only by the authorized personnel for the purposes of the processing on a need to know basis. Access is granted only if there is a clearly specified administrative purpose, and only to those whose role and level of responsibility require them to have access. HR staff having access to the data is bound by confidentiality.

Forms are collected in the data subject's personal file, which is kept in line with the applicable retention period.

Electronic archives are kept in INEA's Human Resources restricted INEA Shared Drive and Functional mailbox and only accessible by designated staff members.

The requests from staff concerning this topic processed via the HR ticketing system are subject to security measures that limit the access to information to the HR staff member(s) in charge and to the Head of Sector and her/his backup. The protection and confidentiality granted to personal data submitted in the ticketing system is the same level of protection and confidentiality granted to secured HR folders. The ticketing system has an additional level of encryption of files attached to tickets that adds up to the file system access control rights. The text of a ticket is contained in a database which has an additional level of authentication that adds up to the file system authentication.

Individual personal files are created and stored in secure archives that are accessible only to authorised personnel. An electronic version of the personal data is stored by the Unit R4 – HR Service and kept confidential with restricted access rights.

All corporate electronic datasets are safeguarded in the Data Center of the Commission, and therefore covered by the numerous defensive measures implemented by DG DIGIT to protect the integrity and confidentiality of the electronic assets of the Institution.

The access to the personal data is protected by the management of the access rights which are strictly limited to specific user groups. The entitlement is distributed according to the principle of 'the need to know' taking into consideration the function, the job and responsibilities of the applicant for an access right. Consequently, the access rights are continuously updated in accordance with the changes in the assignments of the jobholders.

The login and the passwords are managed by the common certification service of the European Commission.

INEA is bound by Commission Decision 2017/46 of 10/1/17 on the security of communications & information systems in the EC.

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/data-protection-0>