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: 2020-022/R4-HR-19
Created on (date): 11/05/20
Last update (date): 10/09/20 Save number: inea.r.r04.r41(2020)5333332

NAME OF THE PROCESSING ACTIVITY

Processing of personal data in the context of whistleblowing

GROUND FOR THE RECORD:

☒ *Regularisation of a data processing activity already carried out*
This record replaces notifications HR 32 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)

No applicable

1.4. Name and contact details of processor (where applicable)

Not applicable

1.5. Purpose of the processing

Whistleblowing procedures provide safe channel for staff or other informants to report fraud, corruption or serious wrongdoings. This is an obligation placed on staff members by the EU Staff Regulations which state that staff members who become aware of a possible illegal activity should report it without delay. In the course of such a procedure, the processing of personal data will be necessary; for example, information relating to those suspected of wrongdoing as well that of the informants and/or other third parties such as witnesses. INEA has clear whistleblowing procedures in place.

The purpose of the processing operation is to establish reporting channels for whistleblowing, manage and follow-up reports and to ensure protection of whistle-blowers in line with the Guidelines on Whistleblowing.

As the whistleblowing arrangements serve as a detection mechanism to bring cases to the attention of OLAF, the duty to report concerns only serious wrongdoings and irregularities. The scope of these Record is limited to the initial stage when INEA receive a report and not when it has been referred or sent directly to OLAF.

The abusive use of the whistleblowing procedure (if the whistle blower maliciously makes a false statement) may lead disciplinary measures.

Whistleblowing procedures contain the processing of sensitive personal information. INEA is required to manage whistleblowing reports and ensure the protection of the personal information of the whistleblowers, the alleged wrongdoers, the witnesses and the other persons appearing in the report.

The application of data protection principles will, inter alia, help creating reliable channels by reinforcing security aspects of the procedure.

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;

Staff Regulations notably (articles 22a to 22c) and corresponding conditions of employment of other servants (article 11). They complement the general principle of loyalty to the European Union, the obligation to assist and tender advice to superiors (Article 21) as well as the rules on how to deal with orders which are considered to be irregular or likely to give rise to serious difficulties (Article 21a).

Communication to the Commission on Guidelines on Whistleblowing – SEC(2012)679 of 6 December 2012.

INEA Steering Committee Decision SC(2018)017 of 26/06/2018 on the adoption of guidelines on whistleblowing.

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

INEA Anti-Fraud Strategy
https://ineanet.inea.cec.eu.int/sites/default/files/sites/default/files/media_files/emop_manual/final_for_publication_inea_2018_afs.pdf

1.7. Categories of data subjects

All staff (CA, TA, interimaires, trainees and consultants), staff of other EU institutions, external stakeholders (contractors of the Agency, beneficiaries of grants managed by the Agency, etc.)

The whistleblowing rules are addressed at staff members who become aware of serious irregularities "in the line of duty". They regard in particular the staff member, who incidentally discovers that something in his/her immediate working environment is going seriously wrong.

1.8. Categories of personal data

The data collected from the whistleblowers concerns facts linked to concerns on fraud, corruption or other serious wrongdoing discover in the line of duty, which may include

- *administrative data (names, professional details, etc)*
- *data relating to suspected offences, criminal convictions or security measures and data relating to the evaluation of personal aspects of the data subject (e.g. abilities, efficiency and conduct)*

Examples of such data may be possible fraud, corruption, embezzlement, theft and serious conflicts of interests in procurement and grant procedures.

The report of the whistleblower may contain personal information of witnesses and third parties (persons merely quoted in the file), the persons against whom the allegations have been made and the whistleblower himself. Therefore, the report itself is also personal information of the whistleblower since it relates to his or her behaviour (as a whistleblower).

On the other hand, the mere fact that a name is mentioned in a document does not necessarily make all the information contained in that document "data relating to that person". In many situations, information can be considered to relate to an individual only when it's about that individual.

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 Commission[2].

[a) Retention period:

Personal information must not be kept for a longer period than necessary having regard to the purpose of the processing. Therefore, different conservation periods should apply depending on the information in the report and how the case is dealt with.

Firstly, personal information that is not relevant to the allegations should not be further processed and is thus deleted.

Secondly, when an initial assessment is carried out but it is clear that the case should not be referred to OLAF or is not within the scope of the whistleblowing procedure the report should be deleted as soon as possible (or referred to the right channel if it for example concerns alleged harassment). In any case, personal information should be deleted promptly and usually within two months of completion of the preliminary assessment, since it would be excessive to retain such sensitive information.

Thirdly, if it is clear after the initial assessment that a report should be transferred to OLAF, INEA should carefully follow what actions OLAF takes. If OLAF starts an investigation it is not necessary for the INEA to keep the information for a longer period. In case OLAF decides not to start an investigation, the information should be deleted without delay.

In case a longer retention period is envisaged, access to the personal information should still be limited (see security measures below). INEA will separate these reports from the main case management system/daily system in use.

INEA applies the retention periods as referred to in points 4.7 and 12.4 of Common Retention List of the Commission, which are

- *15 years for data on OLAF investigations (Protection of EU financial interests)*
- *15 years in case of administrative investigations*
- *20 years in case of disciplinary measures .*

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

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

retention period in point 1.9 a).

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

1.10. Recipients of the data

On a need to know basis:

- *Immediate superior,*
- *Director (AIPN),*
- *Chair of the Steering Committee (in case of appeal during a reclassification exercise),*
- *Ethics Correspondent,*
- *Legal adviser,*
- *INEA OLAF correspondent*
- *OLAF in case of an investigation conducted in application of Regulation (EC) No 1073/1999 and in application of Article 8 of Regulation N° 883/2013 refers to the obligation to transmit to OLAF "without delay any information relating to possible cases of fraud, corruption or any other illegal activity affecting the financial interests of the Union".*
- *Investigation and disciplinary Officer of the Commission (IDOC) and Disciplinary Board members in case of administrative investigations and/or disciplinary measures*

In case of audits or proceedings, etc., INEA's Internal Controller, Legal Team, DPO, 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;*
- *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 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

INEA has in place appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal information to be processed.

In the context of whistleblowing, ad hoc security measures are in place to effectively prevent personal information from being accessed by non-authorised persons and to guarantee its integrity.

The anonymous letterbox allowing whistleblowers to report fact is locked and may only be accessed by the Ethics Correspondent.

Documents are stored in a safe and may only be retrieved by the Ethics Correspondent. The IT sector has a sealed envelope with the code and the person who can have access to it in case of. All confidential electronic documents are protected by a password. The Ethics Correspondent is the only one having the password and the IT sector has a sealed envelope with the code and the person who can have access to it in case of the need.

The identity of the whistleblower who report serious wrongdoings or irregularities in good faith is treated with the utmost confidentiality as they should be protected against any retaliation. Their identity is never revealed except in certain exceptional circumstances if the whistleblower authorises such a disclosure, if this is required by any subsequent criminal law proceedings, or if the whistleblower maliciously makes a false statement.

The person against whom an allegation has been made is protected in the same manner as the whistleblower, since there is a risk of stigmatisation and victimisation within their organisation. They will be exposed to such risks even before they are aware that they have been incriminated and the alleged facts have been analysed to determine whether or not they can be substained.

Therefore, internal access to the information processed as part of the investigation of the allegations is granted strictly on a need to know basis, that is, subject to the necessity to have access.

Personal data is stored electronically and in paper and accessible only by the Ethics correspondent for the purposes of the processing. Further access to data is granted only to those whose role and level of responsibility require them to have access.

The Ethics correspondent and all data recipients are subject to a duty of discretion and bound by confidentiality in the exercise of the functions.

The access to electronic files is protected by the management of the access rights which are strictly limited to specific user or group of users. 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.

Any transmission of data between data recipients will be done using strict confidentiality procedures. For paper files transmission will only be done in hand and in closed envelopes and for electronic files only via secured encrypted e-mail (SECEM).

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/legal-issues/data-protection