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: 2020-023/R4-IT-1
Created on (date): 13-02-2019
Last update (date): 17.07.20

NAME OF THE PROCESSING ACTIVITY

INEA IT support and access management

GROUND FOR THE RECORD [*TICK THE RELEVANT ONE*]:

☒ *Regularisation of a data processing activity already carried out*
This record replaces notifications IT 1 & 2 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[2]

1.1. Name and contact details of controller

a. INEA Unit R4

Chaussée de Wavre 910

W910

BE – 1049 Brussels

b. the Head of Unit R4

c. Email: INEA-IRM@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)

DG DIGIT under

- Service Level Agreement DIGIT-042-00 for the provision of IT Services

- Memorandum of Understanding for ICT Procurement services provided by DIGIT to INEA

- Memorandum of Understanding for the "FPFIS-CMS" SERVICE between INEA & DIGIT

1.5. Purpose of the processing

Personal data is processed to perform the following tasks:

- Manage authentication & authorization of end users to give them access to IT infrastructure critical to their job
  - Desktop computer systems and printers
  - Corporate email accounts
  - Local data repositories (network storage systems, collaboration spaces)

  Processing for this task ends when the staff member (data subject) leaves INEA.
- Manage IT helpdesk support with regard to
  - requests for IT equipment, repairs and configuration of existing equipment
  - interventions by the local IT Helpdesk
  - GIS service (map) requests
  - IT development requests
  - Logistics requests

[2] *This part of the record will be published on INEA website and should be aligned with the information provided in the DP notice*

  - Reporting request
- Manage the IT equipment loans, and protect IT assets from theft or loss, personal data are stored in both a paper form and electronically in the GLPI system.
  Processing for this task ends when the loaned item is returned. No further processing happens after the return of the item.

1.6. Legal basis for the processing

- Council Regulation 58/2003 of 19 December 2002, laying down the Statute for executive agencies to be entrusted with certain tasks in the management of EU programmes;
- Regulation (EC) n° 1653/2004 of 21 September 2004 on a standard Financial Regulation for the executive agencies pursuant to Council Regulation (EC) n° 58/2003 of 19 December 2002 laying down the statute for executive agencies to be entrusted with certain tasks in the management of Community programme;
- Commission Decision 2013/801/EU of 23 December 2013 establishing the Innovation and Networks Executive Agency and repealing Decision 2007/60/EC establishing the Trans-European Transport Network Executive Agency as amended by Decision 2008/593/EC
- Commission Decision 2017/46 on the security of communication and information systems in the European Commission
- EC guidelines for the use of IT equipment & services
- INEA_IT_Mobile Policy

1.7. Categories of data subjects

The following categories of data subjects are identified:

- INEA Staff registered in the above-mentioned IT systems including statutory (temporary & contractual) agents, trainee, interim and external service providers (intra-muros).

1.8. Categories of personal data

- username
- first name and last name
- office address/number
- telephone number (business)
- e-mail address (business)

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

[a) Retention period:

IT helpdesk support

IT helpdesk ticket system data retention period is equal to the full site backup data retention (based on the INEA backup policy).

Access/authentication:

- Personal data is stored in the corporate IT system, for corporate applications see DPO 839 on "Identity Management Services". The data managed by INEA is automatically deleted by the corporate systems upon change/termination of employment of the staff member.
- Any request for access in paper format are retained for 5 years after the end of the employment of the staff member,

Management of the IT equipment loans

- Paper files are kept for maximum one year after the item's return
- Electronic data retention period is equal to the full site backup data retention (based on the INEA backup policy).

Back-ups of files: according to INEA backup policy, the offsite full backup data of all locally managed data is kept for maximum 5 years. Incremental and daily backups are only retained for 1 month.

b) Storage period:

Same as per retention period above

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

- IT helpdesk staff (internal)
- Logistics helpdesk (internal)
- GIS team (internal)
- IT development team (internal)
- INEA reporting team (internal)
- INEA management (internal) – aggregated data only – no personal data at individual level

In case of audits or proceedings only the Internal Controller, Legal Team & DPO of the Agency

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;*
- *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;*
- *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

The personal data of users is collected from three different sources:

- The European Commission active directory services (read-only access);
- The INEA ticket system and the loans management system, internal applications
- Paper forms (IT equipment loans, Request for access to information systems or IT resources).

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. IT staff having access to the data is bound by confidentiality.

Electronic information is stored in networks drives, whose access is governed by the access rights policy of INEA. By default the information is classified "internal" for INEA staff. Folders with limited or confidential information are marked as "restricted area" of "confidential" and they are accessible only by the authorised users.

Access to personal data is restricted on an individual need to know basis. Electronic data is password protected and resides on servers of the European Commission, which implement adequate security measures to protect the security and integrity of the relevant electronic assets. 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.

Only the system administrators can operate the daily/monthly back-ups.
The data of the offsite full back-up is stored in tapes kept in a safe at INEA's premises.
The data of the normal back-ups is directly kept in the robot in the servers' room. Only the system administrators can operate the daily/monthly backups. The system

administrators are statutory staff bound to the rules of staff regulations on good administrative behavior.

Local INEA applications reside within the European Commission's network boundary so they are subject to the same protection as corporate systems.
Paper records are stored in the secured premises of INEA (locked room/cupboard).

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/ict/ict-support*