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: 2019-005/C05-PROG-05
Created on (date): 30.04.19
Last update (date): 25.09.20

NAME OF THE PROCESSING ACTIVITY

Processing personal data through the WiFi4EU Portal

GROUND FOR THE RECORD:

☒ *Regularisation of a data processing activity already carried out*
☐ *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[3]

1.1. Name and contact details of controller

a) Innovation and Networks Executive Agency (INEA) – Unit C5
Chaussée de Wavre 910
W910 04/136
BE – 1049 Brussels

b) the Head of Unit

c) Email: INEA-CEF-WiFi4EU@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)

a) DG Communications Networks, Content and Technology (DG CONNECT) - Unit B5
Avenue de Beaulieu 33
B-1160 Brussels / Belgium

b) the Head of Unit

c) Email: CNECT-B5@ec.europa.eu

WiFi4EU Helpdesk:
https://europa.eu/european-union/contact/write-to-us_en

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

DESIS framework contract for development, contracted by Commission services.

1.5. Purpose of the processing

The purpose of the processing operations is to allow the European Commission (DG CONNECT) and INEA (the joint controllers) to process personal data of representatives of eligible entities and Wi-Fi installation companies to award, manage and follow-up grants awarded in the context of the WiFi4EU initiative. This also implies the processing of personal data for activities such as: sending newsletters and other communication measures related to WiFi4EU and connectivity; analytics and reporting on the WiFi4EU scheme; managing queries via the WiFi4EU helpdesk (https://europa.eu/european-union/contact/write-to-us_en) and via EU Survey (https://ec.europa.eu/eusurvey/home/welcome).

The aim of the WiFi4EU initiative[1] is to provide citizens and visitors of local communities (end-users) with free, easy and quality Wi-Fi connectivity, and a quick access to local e-services (eGovernment, eTourism, eHealth, etc.) in 6,000 to 8,000 municipalities in Europe by 2020, in order to better integrate them in the Digital Single

Market. The data processing operations aim to select WiFi4EU beneficiaries and Wi-Fi installation companies, award, manage and follow-up grant contracts, communicate about the WiFi4EU initiative. Therefore potential beneficiaries and Wi-Fi installation companies provide information, including personal data, through the WiFi4EU portal and this information will be processed by the European Commission and INEA to implement the initiative.

More specifically, INEA is responsible for the data processing operations linked to the following steps: publication and launch of the calls as well as registration, application, selection, evaluation, award, payment and contract management of the WiFi4EU initiative. As authorizing officer, INEA notifies the legal representatives of the applicants (data subjects) about all relevant steps. On the other hand, the Commission is the portal owner and is responsible for the initiative from a policy point of view and may process personal data in the course of the verification of the call's results (e.g. list of winners and list of eligible entities), communication with the applicants and beneficiaries in relation to the calls, and for monitoring and auditing the implementation of the initiative. The Commission accesses the WiFi4EU portal's back office, including personal data of municipalities and suppliers for two major reasons: verifying the implementation during the call launches and evaluations, and for communication purposes when there is a specific communication case, such as interview/success story or an external request for information. The list of registered Municipalities will be made public on the WiFi4EU portal. Besides, the registered Municipalities will have access to information about registered Wi-Fi installation companies declaring they can operate in their area and vice versa. [1] https://ec.europa.eu/digital-single-market/en/policies/WiFi4EU-free-wi-fieuropeans

1.6. Legal basis for the processing

The legal basis for the processing activity is Article 5.1 (a) and (c) of Regulation (EU) 2018/1725.

The legal framework is:

- Regulation (EU) 2017/1953 of the European Parliament and of the Council of 25 October 2017 amending Regulations (EU) No 1316/2013 and (EU) No 283/2014 as regards the promotion of internet connectivity in local communities.
- 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 establishing the Trans-European Transport Network Executive Agency 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;
- Commission Decision (2018) 1281 final of 27.2.2018 on amending Decision C(2013)9235 delegating powers to the Innovation and Networks Executive Agency, as regards promotion of internet connectivity in local communities

Personal data are processed because it is necessary for the performance of a task carried out in the public interest, namely the management of the WiFi4EU Initiative as laid down by Regulation (EU) 2017/1953 of the European Parliament and of the Council of 25 October 2017 amending Regulations (EU) No 1316/2013 and (EU) No 283/2014 as regards the promotion of internet connectivity in local communities. Personal data are necessary to select beneficiaries, award the vouchers and manage contracts.

The processing of personal data is necessary for the performance of a contract to which the data subject is party, namely a grant agreement in the context of the WiFi4EU initiative.

1.7. Categories of data subjects

The categories of data subjects are:

- Representatives of registered Entities that are Applicants and / or Beneficiaries (legal representative or contact persons);
- Representatives of Wi-Fi Installation Companies.

1.8. Categories of personal data

The categories of personal data for registered entities/applicants/beneficiaries are:

- First name
- Last name
- Official address
- Organisation/Department
- Position/Function
- E-Mail address
- Telephone
- Copy of ID/passport* or any document that can replace it, such as a driving licence
- Copy of signature (in case of Assigned Signatory form)

*A copy of ID/passport is required in the application in order to verify that the name and the surname of the legal representative of the Registered Municipality / Applicant / Beneficiary do correspond to the information already provided in the forms filled in the registration phase. In cases requiring investigation, INEA may also verify during the admissibility and eligibility checks and the grant agreement management that the signature on the ID/passport is the same as the one appearing in the scanned form. Therefore, the minimum requirements are that the name of the legal representative, the document number and signature are readable/visible on the copy of ID/passport. Data subjects are requested to erase or make illegible the remaining personal data before uploading the copy of the ID/passport on the WiFi4EU Portal.

For the purposes of registration in the Portal and participation in the call for proposals, the provision of personal data of at least one staff member or representative of registered entities/Applicants/Beneficiaries/Wi-Fi Installation companies as described in the present data protection notice is mandatory.

- Language
- ECAS ID

The categories of personal data for Wi-Fi Installation companies are:

- First name
- Last name
- Official address
- Organisation/Department
- Position/Function
- E-Mail address
- Telephone
- Financial identification for payment
- Language
- ECAS ID

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

a) Data are kept only for the time necessary to fulfil the purpose of collection or further processing.

For information on beneficiaries receiving EU funding, personal data included in application/grant management related documentation are retained for 10 years after the closing of the action, as stipulated in the Common Commission-Level Retention List (CRL, ref. SEC(2019)900). This retention period is considered as necessary for control and audit purposes.

In line with this retention list, personal data related to registration alone or unsuccessful applications are kept for 5 years after the award decision has been adopted for the specific call.

b) Processing of personal data for statistical purposes takes place.

During all the operations, information is kept in an identified data warehouse (located within EU), so that reports, statistics and analytics can be produced in an appropriate visualization format. Reports are produced as required for monitoring the progress on the implementation of the WiFi4EU Initiative, in order to fulfil the Controllers' legal obligations, including to respond to any Parliamentary questions, investigations from OLAF, and audits from the European Court of Auditors, etc. In addition, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. In such cases these personal data are clearly identified.

1.10. Recipients of the data

Access to personal data is provided only to the Commission and INEA staff responsible for carrying out this processing operation and to authorised staff according to the “need to know” principle. Such staff abide by statutory rules, and when required, additional confidentiality agreements.

The other categories of recipients are:

- IT Developers of contractors responsible for developing the portal and helpdesk officers of contractors responsible for the management of the helpdesk, who act as processors on behalf of the Commission.

Data may also be transferred to the following entities in the framework of a particular inquiry in accordance with Union law, which shall not be regarded as recipients per se: Commission services in charge of ex-post controls, without prejudice to a possible transmission to the bodies in charge of a monitoring or inspection task in accordance with European law (OLAF, European Court of Auditors, Ombudsman, EDPS, IDOC, European Court of Justice, the Internal Audit Service of the Commission and EPPO).

Personal data may be registered in the Early Detection and Exclusion System by the Commission, should the beneficiary be in one of the situations mentioned in Articles 136 and 141 of Regulation (EU, Euratom) 2018/1046

For more information, please visit:
http://ec.europa.eu/budget/explained/management/protecting/protect_en.cfm.

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

No transfers to third countries or international organisations are foreseen.

1.12. Description of security measures

All personal data in electronic format (e-mails, documents, databases, uploaded batches of data, etc.) are stored on the servers of the European Commission (DIGIT data center). All processing operations are carried out pursuant to the Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission. Personal data are not transferred to third countries.
The Commission's contractors are bound by a specific contractual clause for any processing operations of your data on behalf of the Commission, and by the confidentiality obligations deriving from the General Data Protection Regulation of their respective EU Member States ('GDPR' Regulation (EU) 2016/679).

In order to protect personal data, the Commission has put in place a number of technical and organisational measures.

Technical measures include appropriate actions to address online security, risk of data loss, 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. Access rights and controls are secured via the EU login with password granted only to those persons authorised to get access to the specific documents (call management, grant management, etc.) necessary for the processing.

1.13. Data Protection Notice

The Data Protection Notice (DPN) relevant to this data processing activity is available on:

- The WiFi4EU Portal: https://WiFi4EU.ec.europa.eu/#/home
- The INEA website: https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/WiFi4EU

- The Europa website: https://ec.europa.eu/digital-single-market/en/news/privacy-statement-WiFi4EU