EUROPEAN HEALTH and DIGITAL
EXECUTIVE AGENCY (HaDEA)

RECORD OF PERSONAL DATA PROCESSING ACTIVITY

*In accordance with **Article 31 of the Regulation (EU) 2018/1725**[1] on the protection of natural persons with regards to the processing of personal data by the Union Institutions, bodies, offices and agencies and on the free movement of such data, individuals whose personal data are processed by the Executive Agency in any context whatsoever are to be protected with regard to the processing of personal data and the Executive Agency has to keep records of their processing operations.*

Therefore, each responsible HaDEA data controller has to maintain a record of the processing activities under his/her responsibility.

In accordance with Article 31 of the data protection regulation, this record covers two aspects:
1. Mandatory records under Art 31 of the data protection regulation (recommendation: make the header and part 1 publicly available)
2. Compliance check and risk screening (initial; part 2 is internal only to the Agency, not published)
The ground for the record is (tick the relevant one):

Record No: - PROG.01 **Initial approval by Data Controller**: ARES registration date

Update (s) *(if applicable):* N/A

NAME OF THE PROCESSING ACTIVITY

WiFi4EU mobile application

IDENTIFICATION OF THE DATA CONTROLLER

European Health and Digital Executive Agency (HaDEA), Head of Unit HaDEA.B.1

GROUND FOR THIS RECORD (*select relevant ground*)

□ Record of a new type of processing activity of personal data (before its implementation)
X Record of a processing activity of personal data that is already in place
□ Change/Amendment/ Update of an already existing previous record

[1] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295/39 of 21.11.2018).

1. INFORMATION ON THE PROCESSING ACTIVITY of WiFi4EU APPLICATION

This processing activity is performed in accordance with **Regulation (EU) No 2018/1725**[2] on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data.

1.1. The Data Controller is:
Head of Unit HaDEA.B.1 European Health and Digital Executive Agency (HaDEA), Place Charles Rogier 16, B-1049 Brussels, BELGIUM and can be contacted at HADEA-CEF-WiFi4EU@ec.europa.eu.

1.2 The contact details of the Data Portection Officer (DPO)

HADEA-DPO@ec.europa.eu

1.3 Joint controller: Not applicable.

1.4 The following entity(ies) is/are acting as Processor(s): Not Applicable

1.5 Description and purpose(s) of this processing :

The aim of the WiFi4EU app (developed in the context of the WiFi4EU initiative) is to provide access to users to locate free WiFi4EU hotspots at locations throughout Europe, of municipalities that have obtained a voucher to install WiFi networks in public spaces such as: cultural and touristic sites, health centres/hospitals, stations and transport stops, schools, universities and libraries, parks and squares, shopping malls, town & sport halls. The app is designed to make it easier for users to find these hotspots and is free of charge to download and use.

To improve user experience and accuracy of the data, users have the option to get in contact with the WiFi4EU team to either: (1) provide feedback or suggestion for improvement for the application or (2) report any issue related to the location, malfunctioning, or any other type of issue on access points, via the dedicated EU Survey pages (accessing the EU Survey will take the user outside of the app interface). Users can voluntarily choose the option to be contacted back by the WiFi4EU team at an email address provided by them to get feedback on their query.

Upon consent, the app may use the user's geolocation to identify hotspots around their current location, without collecting this information. Specifically, users will be asked if they wish to be geolocated, which will help improve their experience. If they agree to be geolocated, their device's location is processed directly on their device. Location data is neither collected, stored or shared by HaDEA (European Health and Digital Executive Agency) or third parties. Refusing geolocation does not prevent users from using the application.

1.6 The legal basis for the processing based on Article 5(1) of Regulation (EU) 2018/1725 is/are:

☐ **(a)** the 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[3] laid

[2] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295/39 of 21.11.2018).

down in Union law;

☐ **(a2)** the processing is necessary for the **management and functioning** of the Union Institutions, bodies or agencies (Recital (22) of Regulation (EU) 2018/1725) laid down in Union law;

☐ **(b)** the processing is necessary for **compliance with a legal obligation** to which the controller is subject, which are …[4] laid down in Union law;

☐ **(c)** the processing is necessary for the **performance of a contract** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

☒ **(d)** the data subject has given **consent** to the processing of his or her personal data for one or more specific purposes[5];

☐ **(e)** the processing is necessary in order to protect the **vital interests** of the data subject or of another natural person.

1.7 The categories of data subjects

☒ Agency staff (Contractual and temporary staff in active position)

☐ Visitors to the Agency

☐ Applicants

☐ Relatives of the data subject

☐ Complainants, correspondents and enquirers

☐ Witnesses

☐ Beneficiaries

☐ External experts

☐ Contractors

☒ Other, please specify:

Users of the WiFi4EU application who are submitting any remarks via the "Report issue" button or via the Helpdesk link.

1.8 Categories of personal data

a) Categories of personal data:

When reporting an issue or providing feedback via EU Survey:

When the user contacts the WiFi4EU team via the "Report issue" button or via the Helpdesk link, he/she will be directed to an external survey hosted on the EU Survey platform. The user may voluntarily provide personal data to report an issue – this data is processed to the extent necessary to

[3] Commission Implementing Decision (EU) 2021/173 of 12 February 2021 establishing the European Climate, Infrastructure and Environment Executive Agency, the European Health and Digital Executive Agency, the European Research Executive Agency, the European Innovation Council and SMEs Executive Agency, the European Research Council Executive Agency, and the European Education and Culture Executive Agency and repealing Implementing Decisions 2013/801/EU, 2013/771/EU, 2013/778/EU, 2013/779/EU, 2013/776/EU and 2013/770/EU.

reply and regular reporting on the activities within the WiFi4EU project. Additional personal data which might be shared by the data subject will be disregarded.
The relevant privacy statement for EU Survey can be consulted at: EUSurvey - Privacy Statement (Record reference: DPR-EC-01488).

b) Categories of personal data processing likely to present specific risks: not relevant

c) Categories of personal data whose processing is prohibited, with exceptions (art. 10): not relevant

d) Specify any additional data or explanatory information on the data being processed, if any:

When activating the geolocation option:

Geolocation: upon consent, the app may process the geolocation of the user to identify hotspots around your current location. Specifically, the user will be asked if he/she wishes to be geolocated, which will help improve teh user's experience. In case of consent to be geolocated the device's location of the user is processed directly on the device. Location data is neither collected, stored or shared by HaDEA (European Health and Digital Executive Agency) or third parties. Refusing geolocation does not prevent the user from using the application.

When the location setting is off for your device, the apps can't get your device's location. The location access options can be changed at any time via the device settings.

1.9 Retention period (maximum time limit for keeping the personal data)

The personal data concerned **will be kept for a maximum period** of 6 months from the time of reporting of the issue through the feedback platform. Data will be deleted at the end of this period.

Is any further processing for historical, statistical or scientific purposes envisaged?
☐ yes ☒ no

1.10 The recipient(s) of the data

The recipients to whom the personal data will or might be disclosed are:

Relevant staff of HADEA in charge of the technical and operational aspects of the WIFI4EU application have access, **on a need-to-know basis,** to address the concerns raised by users.

- In case of audits or proceedings, etc., HaDEA's Internal Controller, Data Protection Officer, Legal Affairs Sector, etc .

- In addition, in case of control or dispute, personal data can be shared with and processed by the bodies charged with a monitoring or inspection task in application of Union law in compliance with the applicable data protection rules and within the scope of their tasks entrusted by the relevant legislation. This includes, in particular, the following recipients:

    - Bodies in charge of a monitoring or an inspection task in application of Union law (e.g. internal audit, IAS, Court of Auditors, etc.);

- 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;
- OLAF in case of an investigation conducted in application of Regulation (EC) No 1073/1999;
- 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 Regulation (EC) 2018/1725;
- 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

Personal data **will not be transferred to third countries** or **international organisations.**

1.12 The processing of this personal data **will not include** automated decision-making (such as profiling).

1.13 Description of security measures

The following technical and organisational security measures are in place to safeguard the processing of this personal data:

The European Commission's IT systems used by the Agency abide by the Commission's security guidelines. The Agency complies with Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission.

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 is 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).

1. Organisational measures:

A Corporate Local Informatics Security Officer (C-LISO) is in place. Its role includes supervising the Agency compliance with the relevant regulations, and the application of security measures recommend by DIGIT.

Organisational measures include appropriate access rights and access control. As a rule within the Agency, access to information systems, the file system or offices are subject to a series of authorisations where the person granting the access is different from the person requesting or authorising the access - except in limited cases of delegation. The responsible person in the unit in

charge of this action (processing operation of the current record) collects and places personal data in electronic format on the secured drive of the Unit with restricted access on a need to know basis. All Agency staff and its contractors are bound by confidentiality obligations. The need to know principle applies in all cases. Moreover, only authorized staff has access rights to consult EU Survey – this is protected by EU Login and appropriate rights to the organisational entity managing the project.

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.

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 (Project Officer/Project Assistant/Project Adviser working on the WiFi4EU initiative, etc.) necessary for the processing.

1.14 Data protection Notice

Data Subjects are informed on the processing of their personal data via a **data protection notice on their rights :**

- to access their personal data held by a controller;
- to request their personal data held by a controller to be corrected;
- to obtain in some situations erasure of their personal data held by a controller, e.g. when data are held unlawfully (right to be forgotten);
- to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
- **of recourse** at any time to the **HaDEA Data Protection Officer** at HADEA-DPO@ec.europa.eu Click here to enter text. and to the **European Data Protection Supervisor** at https://edps.europa.eu.

Request from a data subject to exercise a right will be dealt within **one month**.

Your right to information, access, rectification, erasure, restriction or objection to processing, communication of a personal data breach or confidentiality of electronic communications may be restricted only under certain specific conditions as set out in the **applicable Restriction Decision** in accordance with Article 25 of Regulation (EU) 2018/1725.