WiFi4EU - Questions and Answers

1. BACKGROUND

1.1. What is the overall aim of the WiFi4EU initiative?

The WiFi4EU initiative aims to provide high-quality Internet access across the EU to citizens and visitors via free of charge Wi-Fi hotspots in public spaces such as parks, squares, administrations, libraries, and health centres. Vouchers funded the European Commission via the initiative will be awarded to support municipalities for the installation of the Wi-Fi hot spots in these centres of public life, using the services of Wi-Fi installation companies.

1.2. Who can participate in the WiFi4EU initiative?

The WiFi4EU initiative is open to public sector bodies from the EU Member States and participating EEA countries (Norway and Iceland). Only the municipalities (or equivalent local administrations) or associations of municipalities may participate. The specific list of entities eligible to apply for the fourth call was agreed by the Member States and is available for reference here: https://digital-strategy.ec.europa.eu/en/news/list-eligible-entities-wifi4eus-fourth-call

Each municipality can only benefit from one voucher during the entire duration of the WiFi4EU initiative. Therefore, municipalities awarded a voucher in a previous WiFi4EU call were not eligible to apply for a later call, whereas unsuccessful municipalities could try again in later calls.

1.3. What is the amount of the WiFi4EU voucher?

The amount of each voucher to be awarded is EUR 15,000.

2. REGISTRATION

2.1. Who are the *municipalities* and *associations formed by municipalities* allowed to register? How and when can we register?

In order to apply for the WiFi4EU initiative, all eligible municipalities (or associations of municipalities) included in the above-mentioned list (Q1.2) must first fill in their registration information via the WiFi4EU Portal (https://wifi4eu.ec.europa.eu/#/home).

Note that an EU Login linked to the municipality must be used for the registration process. (For more information about creating an EULogin, see: https://webgate.ec.europa.eu/cas/manuals/EU_Login_Tutorial.pdf).

Go to the homepage of the WiFi4EU Portal to begin the registration. Then, select your municipality from the drop down list. Provide the required information about the municipality (including country, type of organization to be registered (municipality or association), address).

Please include the contact information for the mayor/head of municipality/legal representative, i.e. the person who has the competence to sign the Grant Agreement. **Attention: we recommend that for the signing of the Grant Agreement this is ONLY the head of the municipality/mayor, and not any legal representative of the municipality.** Should the mayor/head of municipality nevertheless wish to nominate a different person to sign the Grant Agreement (i.e. an "Authorised Person"), this "Authorised Person's" contact information should also be included in the registration.

Please note that the access to the Portal is **always** linked to the person, including his/her email address, who created the EU Login during the registration process and who is therefore indicated as the "Contact Person" in the Portal. Therefore, we strongly advise that if you wish to include an "Authorised Person" in your application, this person is the same as the "Contact Person" (including the email address indicated) to facilitate the process of signing the Grant Agreement.

"*Associations of municipalities*" may register multiple municipalities in order to simplify the management of those registrations. However, each association will be required to separately submit the final application online for each municipality included in its registration. Note that associations of municipalities are not entitled to receive a voucher; each voucher is awarded to an individual municipality as the beneficiary.

In all cases, only the name of the registered municipality will be made public. (See Q8.1 about data protection).

Municipalities do not need to include with their registration (or application) any technical descriptions or documentation about the Wi-Fi network to be deployed. Preliminary assessments of any project costs (e.g. estimates from Wi-Fi installation companies) are also not required.

2.2. We are a Wi-Fi installation company. How and when can we register? How do we modify our data?

Wi-Fi installation companies are encouraged to participate in the WiFi4EU initiative. A list of registered Wi-Fi installation companies is available on the WiFi4EU Portal. Municipalities may consult this list if they are awarded a voucher and are looking for Wi-Fi installation companies in their area which could provide the relevant services.

Wi-Fi installation companies should register on the WiFi4EU Portal to express interest. Go to the homepage of the WiFi4EU Portal to begin the registration. Provide information about countr(ies) and region(s) of operation, as well as the company's contact and bank details.

Please do not register your company more than ONCE in the Portal. If you are not able to access or modify your registration, contact the helpdesk https://europa.eu/european-union/contact/write-to-us_en.

Wi-Fi installation companies may register on the WiFi4EU Portal at any time. However, they must be registered in the Portal if a selected municipality has contracted them to carry out the installation of

its WiFi4EU network in order for them to be able to submit the required information on the implementation of the network once the project is completed.

2.3. How can I edit/update my municipality's registration data in the Portal?

Municipalities may modify almost all of their own data registered in the Portal at any time, *except* during the short period when a call is open and – for the winning municipalities - the time between their signing and INEA's countersigning of the Grant Agreement. These edits may include e.g. updating of the mayor/head of municipality/legal representative's name and/or e-mail address following municipal elections or internal changes in the organisation, or modifications to the contact person's name and/or address, supporting documents, etc.

The only data that may not be directly edited/updated by the municipality is the e-mail address of the person who originally made the municipality's registration in the Portal, because it is linked to the EU Login of the contact person. However, you may request the Health and Digital Executive Agency (HaDEA) to take care of this update/change of the contact person's e-mail address via the following procedure:

1. Send an e-mail to HADEA-CEF-WIFI4EU(AT)ec.europa.eu with the subject line "CONTACT PERSON UPDATE".
2. Include the following information:
    - Municipality name
    - Country name
    - Existing contact person's e-mail address as visible in the WiFi4EU Portal
    - New contact person's e-mail address + name & surname

(Note that it first must be registered in EU Login. For more information about creating an EU Login, see: https://webgate.ec.europa.eu/cas/manuals/EU_Login_Tutorial.pdf).

By sending the above-mentioned request, municipalities confirm that the information provided in the email is correct and as such will be used for any relevant WiFi4EU-related correspondence/follow-up as needed.

The Health and Digital Executive Agency (HaDEA) will make the necessary changes upon your request and inform you directly once they are finalized.

3. APPLICATION

3.1. We are a municipality. How and when can we apply?

In order to apply for a WiFi4EU call, municipalities must first register on the WiFi4EU Portal using a valid EU Login account.

After the call is open, municipalities will then be able to apply for the call by clicking the "Apply for voucher" button on the "My application" page of the Portal.

3.2. What documents are required for application?

In order to be able to apply, municipalities must first complete their registration by uploading to the WiFi4EU Portal the following two required supporting documents:

1. The complete "Proof of agreement" form, including a copy of the legal representative/mayor/head of municipality's passport or ID.

2. The copy of an act of nomination or document establishing that the legal representative (mayor/head of municipality) legally represents the municipality.

If the legal representative wishes to mandate a person to sign the Grant Agreement on his/her behalf, the following two additional documents must also be supplied at the latest before signing the Grant Agreement:

- the "Authorised Person" form, signed by both the legal representative (i.e. mayor/head of municipality and by the authorised person who will sign the Grant Agreement.
- a copy of the Authorised person's passport/ID

The "Proof of agreement" and "Authorised Person" forms are available in all Member State languages from the WiFi4EU Portal under the "My registration" page.

All templates of the supporting documents are available on the WiFi4EU webpage of the Health and Digital Executive Agency (HaDEA) :https://hadea.ec.europa.eu/programmes/connecting-europe-facility/wifi4eu_en. Once completed, they must be uploaded as separate files in the WiFi4EU Portal under the "My registration" page, using a suitable format (.pdf, .png, or .jpg).

3.3. Is it possible to start work on our Wi-Fi network now and, if we get awarded a voucher, redeem it in the future?

Pursuant to the EU Financial Regulation (see https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32018R1046), no grant may be awarded retroactively for actions already completed. In other words, an installation which has been fully completed and delivered before the signature of the Grant Agreement would not be entitled to receive a voucher.

4. SELECTION AND AWARD

4.1. How will the beneficiaries of a voucher be selected?

Municipalities will be selected on a first-come, first-served basis based on the date and time of the submission of their application (i.e. the time they pressed on the apply button in the Portal and NOT the submission date and time of their registration).. See section 7 of the call text for more information about the selection process.

4.2. I cannot sign the Grant Agreement. What should I do?

Signing of the Grant Agreement may be blocked in exceptional cases due to the way the registration was done in the Portal.

For example, if the email address of the mayor/head of municipality/legal representative is the same as the contact person's email address but the names of mayor and contact person are different, the signing of the Grant Agreement may not be possible. To rectify this, the easiest solution is that the municipality changes the e-mail address of the mayor (see Q2.3 above). Alternatively, it may authorize the contact person to be able to sign the Grant Agreement.

If you are having specific IT/technical issues, please contact the Helpdesk with an explanation of the problem and include screenshots as relevant.

4.3. How does the reserve list work?

In case additional funding would become available for a given call, and if a municipality is on the reserve list for that call and the reserve list is still valid, the municipality may still be invited to sign a Grant Agreement.

In practice, this means that if one applicant from the main list drops out, an applicant from the reserve list is selected using both the first come, first served and geographic balance principles as indicated in the selection criteria (section 7) of the call text.

All reserve list applicants will be informed by e-mail in due time if there is still budget available and there is a possibility to sign a Grant Agreement.

4.4. Can I withdraw from the WiFi4EU initiative even after my Grant Agreement has been signed?

Yes, even after a municipality has signed the Grant Agreement in the WiFi4EU Portal, it may still decide to withdraw from the WiFi4EU initiative. In this case, the municipality must notify the Health and Digital Executive Agency (HaDEA) (via HADEA-CEF-WiFi4EU@ec.europa.eu) and provide an official letter signed by the mayor, which clearly states the reasons of the withdrawal. The Health and Digital Executive Agency (HaDEA) will then process the withdrawal and inform the municipality accordingly.

5. IMPLEMENTATION & OPERATION (note for specific technical issues, see also section 9)

5.1. Our municipality was awarded a voucher and our Grant Agreement has been signed by both our municipality and the European Commission/ The Innovation and Networks Executive Agency (INEA). What do we do next?

The municipality must ensure that the installation is completed and the installed network starts working within 32 months (for Calls 1, 2 and 3) and within 24 months (for Call 4) from the countersignature of the Grant Agreement.

First, the municipality must select a Wi-Fi installation company to carry out the work. (Note that the selected Wi-Fi installation company must also register in the Portal – see Q2.2)

Each municipality may contract the Wi-Fi installation company of its choice to install the wireless equipment. Please note that the Commission/the Executive Agency will not intervene in the contractual relationship between the municipalities and their Wi-Fi installation company.

Municipalities will designate 'centres of public life' where the WiFi4EU hotspots will be installed. The Wi-Fi hotspots should be installed in the areas where no similar offers of free Wi-Fi connectivity already exist.

Municipalities are responsible for financing the Internet subscription and maintenance of the equipment in order to offer free and high-quality Wi-Fi for their citizens and visitors for at least three (3) years after the installation of the network.

Municipalities should also clearly display the WiFi4EU visual identity in public spaces offering a WiFi4EU connection to the Internet. More information about the visual identity rules, as well as the WiFi4EU emblem/logo, is available on the WiFi4EU webpage of the Health and Digital Executive Agency (HaDEA):https://hadea.ec.europa.eu/programmes/connecting-europe-facility/wifi4eu_en.

Consult section 6.2 of the call text for more information about the specific technical requirements of the initiative.

5.2. What is the voucher intended to cover?

The WiFi4EU voucher is a lump sum payment intended to cover only the equipment and installation costs of Wi-Fi hotspots meeting the requirements defined in the call text and the Grant Agreement Annex I signed with the selected municipalities.

The equipment includes those items necessary for the deployment of the WiFi4EU network, such as power supply devices (e.g. Power over Ethernet (PoE) adapter, power adapter, PoE switch) or equipment to connect to Internet (e.g. routers, switches, firewalls). However, the main objective of the voucher must be the Access Points, and respecting the required minimum number of Access Points to be installed (see also Q9.2).
Municipalities may also choose to lease the equipment with the option to purchase.

The municipalities will be responsible for the costs of the connectivity (Internet subscription), maintenance and operation of the equipment for at least three (3) years.

See also section 6 below for specific details on payments.

5.3. What is the voucher not intended to cover?

Equipment to extend the backhaul connectivity from another location to the WiFi4EU location is not covered by the voucher. The Internet connection should already be available at the place of deployment and the municipality is responsible for its maintenance for three years.

5.4. Can the project be broader than what is funded by the voucher? I.e. Is it possible to connect multiple centres of local public life?

Municipalities may use the WiFi4EU voucher to partially fund a project of higher value; therefore any equipment and installation costs beyond the value of the voucher would fall under the contract between the supplier and the municipality.

For example, it would be possible to connect several centres of local public life with one network (single captive portal) or several networks (different captive portals). However, if the costs for equipment and installation exceed the value of the voucher, the additional costs would need to be financed by the municipalities or by other national/regional funding sources.

5.5. Will existing public Wi-Fi networks be able to join the WiFi4EU initiative?

Existing public Wi-Fi networks will be able to join the WiFi4EU initiative, provided they respect the conditions and technical specifications described in the Annex I of the Grant Agreement, with a view not to alter the WiFi4EU main features, e.g. the access should be free of charge, without discriminatory conditions and would need to respect the branding requirements.

It will be also possible for existing networks to join the WiFi4EU initiative without using vouchers. We are working towards providing adequate solutions to the different situations that could be presented.

5.6. What is meant by the "minimum 30Mbps download speed" that the WiFi4EU networks should provide?

The WiFi4EU networks should be capable of providing a high quality experience for all end users. Therefore, all winning municipalities must respect the conditions as indicated in section I.3 of the Grant Agreement: "the beneficiary shall subscribe to an offer equivalent to the highest speed available mass-market Internet connection in the area and in any event to one offering at least 30 Mbps download. The beneficiary shall also ensure that this backhaul speed is at least equivalent to that – if any – which is used by the beneficiary for its internal connectivity needs."

In order to check the compliance with the above contractual requirement, Phase II of the WiFi4EU implementation (see FAQ 9.4), planned for 2020, will allow monitoring of the quality of service requirements of WiFi4EU Access Points, pursuant to article I.3 of the Model Grant Agreement. For each network, the total cumulative speed of all Access Points (minimum 10) must be at least 30

Mbps. Municipalities are encouraged to ensure the highest speed possible in the interest of the end users and in line with the connectivity targets set by the European Commission (Recital (2) of Regulation (EU) 2017/1953 – see https://eur-lex.europa.eu/eli/reg/2017/1953/oj).

5.7. What happens if the value of 30 Mbps download speed cannot be guaranteed?

According to the Annex I/article I.3 of the Grant Agreement, the municipality shall subscribe to a mass-market Internet connection offer equivalent to the highest speed available in the area, and ensure that this backhaul speed is at least equivalent to that (if any) used by the municipality for its internal connectivity needs and in any event to one offering at least 30 Mbps download. This requirement is therefore intended for the backhaul Internet connection, not per user. The backhaul connectivity reaching a 30 Mbps should be reached within 32 months (for Calls 1, 2 and 3) and within 24 months (for Call 4) from the countersignature of the Grant Agreement. Temporary degradations of speed due unexpected circumstances are accepted, but will be monitored and reported systematically. Degradation of speed should not be the consequence of reduced backhaul speed. The aim is not just to have a free Wi-Fi connection, but one that is fast and efficient.

5.8. What is "free access"?

As stated in recital (4) of Regulation (EU) 2017/1953 (see https://eur-lex.europa.eu/eli/reg/2017/1953/oj), the service provided by the WiFi4EU hotspots should be free of charge, i.e. “provided without corresponding remuneration, whether by direct payment or by other types of consideration, such as commercial advertising or the provision of personal data for commercial purposes” for the three (3) first years of operation.

Any advertisement on the captive portal (i.e. the municipality's web page that is displayed to newly connected users) constituting a source of revenue for the municipality or the obligation, for end users, to buy any product or service to access the network, would not qualify as “free of charge” in the meaning of this Regulation.

5.9. What is the validity of the WiFi4EU voucher?

The validity period of the WiFi4EU voucher starts on the date of the counter-signature of the Grant Agreement by the European executive agency and it expires at the end of the implementation period.
The initial implementation period was 18 months; it has been extended twice to mitigate the impact of the Coronavirus pandemic on the deployment of WiFi4EU networks, leading to a 32 months implementation period for Calls 1, 2 and 3 beneficiaries; and to 24 months for Call-4 beneficiaries. All implementation deadlines are to be found on the website of the Health and Digital Executive Agency (HaDEA) here: https://hadea.ec.europa.eu/programmes/connecting-europe-facility/wifi4eu/deadlines-wifi4eu-beneficiaries_en

Beyond this maximum implementation period, the voucher validity expires and Wi-Fi installation companies will no longer be able to redeem it.

5.10 What happens if the WiFi4EU network is not notified within the implementation deadline?

All implementation deadlines are to be found on the website of the Health and Digital Executive Agency (HaDEA) here: https://hadea.ec.europa.eu/programmes/connecting-europe-facility/wifi4eu/deadlines-wifi4eu-beneficiaries_en After passing theimplementation deadline, neither the Wi-Fi Installation Company can submit the Installation Report, nor the municipality can approve the Installation Report in the WiFi4EU Portal. The voucher cannot be paid as the project was not completed within the implementation period foreseen in the Grant Agreement.

In accordance with Article II.25.4 of the Grant Agreement, a first formal notification informs one month in advance both the municipality and the selected Wi-Fi Installation Company about the implementation deadline, highlighting that the payment of the voucher will not be executed unless the municipality approves the Installation Report before the implementation deadline. After the implementation deadline is passed, a second formal notification is sent to inform both the municipality and the selected Wi-Fi Installation Company that the WiFi4EU voucher is lost.
Should either the municipality or the Wi-Fi Installation Company not have received any of the two formal notifications, please inform without delay the WiFi4EU Team by email at HADEA-CEF-WIFI4EU@ec.europa.eu.

5.11. Are there any security features applicable to the WiFi4EU networks?

Some security features will be part of the technical specifications of the equipment and detailed in the Grant Agreement, notably in its Annex I. Ultimately, the municipalities will be responsible for managing each WiFi4EU network at the local level and thus define the security settings in line with EU and national law.

In the initial stage, the public WiFi4EU hotspots will not be required to be encrypted. However, it is foreseen that in the second stage, a common authentication platform will be created that will provide additional security features for the connection of end users, as well as facilitate seamless roaming between WiFi4EU hotspots in different areas.

5.12. What is our deadline to select the installation provider?

Municipalities have 32 months (for Calls 1, 2 and 3) or 24 months (for Call 4) to implement the project according to the Grant Agreement. Note that within this 32-month (for Calls 1, 2 and 3) or 24-month (for Call 4) implementation period there is no deadline to select the installation company. However, it is strongly recommended that municipalities make the selection in the WiFi4EU Portal as soon as possible in order to meet the final implementation deadline, and to allow for other important steps that need to be completed before this deadline.

6. PAYMENT

6.1. How can the voucher be redeemed, i.e. what are the steps involving the payment to the Wi-Fi installation company?

In order for the Wi-Fi installation company to redeem the voucher of EUR 15,000 from the European Commission it must have completed all of the following steps and in this order:

1. The installation company must be registered on the WiFi4EU Portal.
2. The installation company must have been designated by a municipality as their provider in the Portal.
3. The installation company must have encoded in the WiFi4EU Portal (in the "Bank account" section "My registration" page) one or more bank accounts complete with all of the relevant details and supporting documents. The sole registration of any bank account does not send the bank account for validation. Point 4 should also be completed.
4. The installation company must have linked (one of) its registered bank account(s) to a municipality for payment. This should be done in the "Bank account" section of the WiFi4EU Portal's "My installation" page, by clicking on "Select bank account". Only then will the Commission commence with the validation of the bank account.
5. The bank account details must have been confirmed by the Commission in the WiFi4EU Portal (see also Q6.5 and Q6.6).
6. The installation company must have submitted an installation report (according to Article 4 of the Grant Agreement), which must subsequently be approved both by the municipality and the Commission in the WiFi4EU Portal.

6.2. Does the voucher cover Value Added Tax (VAT)?

The voucher is a lump sum contribution intended to cover the implementation of the action. The Health and Digital Executive Agency (HaDEA) will not look into the eligibility of actual costs incurred, including Value Added Tax (VAT). As also indicated in Q6.3 below, any costs above the 15,000 EUR value of the voucher (whether or not VAT is included) have to be covered by the municipalities themselves.

6.3. What happens if the cost of the installation is more or less than €15,000?

Pursuant to Article 4 of the WiFi4EU call text, the amount of each voucher to be allocated is €15,000 in the form of a lump sum. Any outstanding balance cannot be covered by the voucher. Any unused contribution must not be returned to the European Commission.

6.4. Can the municipality mandate the setup of the network to several third parties and therefore request a split of the voucher to several Wi-Fi installation companies?

The WiFi4EU vouchers only cover the purchase of the Wi-Fi Access Point equipment and installation. The voucher amount can only be paid to a single Wi-Fi installation company identified by the municipality in the Portal for this purpose. Note that the selected Wi-Fi installation company may outsource or delegate part of the tasks to other companies. In this case, it is the municipality's

responsibility to manage, keeping in mind that the payment will only be made to the original installation company it selected.

6.5. What is the process for the bank account validation of the Wi-Fi installation company?

After a Wi-Fi installation company has been selected by a municipality, it must:

1) encode the bank information for the account in which they would like to receive the payment (in the "Bank account" section of the WiFi4EU Portal's "My registration" page – see also Q6.6), and
2) attach the appropriate supporting documents.
3) Link in the WiFi4EU Portal the bank account in which the company would like to receive the payment with the municipality for which they are making/have made the installation (see also Q6.1 point 4)

Once encoded, and only after the installation company has linked in the WiFi4EU Portal the bank account in which they would like to receive the payment with the municipality for which they are making/have made the installation, both the bank information and the supporting documents are validated through a series of checks by the Commission services. The validation process will only start when the Wi-Fi installation company has earmarked a specific bank account to at least one municipality for payment. The Wi-Fi installation company is then notified by e-mail of the successful validation as soon as all of the checks have been satisfactorily completed. If any additional information is required to complete the validation process, the Wi-Fi installation company will be contacted by e-mail accordingly. The Wi-Fi installation company can also monitor this status via the "My registration" page of the Portal.

6.6. How should we fill out the bank account details on the WiFi4EU Portal and what data should be encoded?

The following data must be encoded in the "Bank account" section of the WiFi4EU Portal's "My registration" page:

- **Account name**: the name in which the account was opened. It can be the same as the account holder but not necessarily (e.g. if it is a shared account, special purpose account). The account name, which is usually found on the bank statement or on another bank document, is the name that should be entered in the Portal.
- **IBAN**: The IBAN (International Bank Account Number) is an account number "formatted" in accordance with international standards which allows banks to perform cross-border transactions between countries.
- **Bank name**: refers here to the final bank, meaning the bank where the account holder keeps the bank account.
- **BIC/SWIFT code**: The BIC (Business Identifier Code) is allocated by SWIFT (Society for Worldwide Interbank Financial Telecommunication) to banks (against payment).
- **Country:** Country where the account is held.

The following data must be entered in the "Account holder details" section of the WiFi4EU Portal's "My registration" page:

- **Street – Street number – City - Country**: refers to the address of the account holder as declared to the bank.

6.7. What is the process for the Wi-Fi installation company to receive the payment?

The Wi-Fi installation company must first have validated bank information in the Portal (see Q6.1 and 6.5). Once the information is valid:

1. The *Wi-Fi installation company* sends the installation report to the municipality for validation via the WiFi4EU Portal.
2. The *municipality* validates the installation report in the Portal, confirming that each encoded Access Point does indeed exist and is placed according to the indicated GPS coordinates.
3. Following the municipality's validation of the installation report, *the Executive Agency* has up to 60 days to:
   a) verify that the Wi-Fi installation is compliant with Article 4.2 of the Grant Agreement (i.e. that there is a running network, displays the WiFi4EU logo etc.)
   b) confirm the quality and reliability of the related information provided in the Portal installation report, and c) make the payment.

In case of non-compliance with Article 4.2 of the Grant Agreement, both HaDEA's confirmation of the installation report and the subsequent payment are suspended for the duration until compliance is ensured. Please also note that it is important to make sure that the installation of the snippet is correct, as otherwise, no payment can be triggered. Consult the Snippet Installation Guide and HTML template, available on HaDEA's's WiFi4EU webpage: https://hadea.ec.europa.eu/system/files/2021-09/cnect-2017-00250-00-11-en-ori-00_0.pdf.

6.8. Should the Wi-Fi installation company invoice the European Commission/ the Executive Agency or the municipality?

The Wi-Fi installation company must invoice the municipality directly. Note that the European Commission/ the Health and Digital Executive Agency (HaDEA) will not intervene in any contracting relations between the municipality and the installation company, and do not need to receive copies of any invoices. Please keep in mind that municipalities and the Wi-Fi installation companies should comply with the national financial rules in terms of invoicing. Municipalities may contact their competent national authority for more information regarding procurement rules, contracting and/or accounting.

Please also note that municipalities should keep all original supporting documents to prove the proper implementation for a period of three years starting from the date of payment of the balance. If there are on-going audits, the documents should be kept until such audits, appeals, litigation or pursuit of claims are closed.

6.9. Can a Wi-Fi installation company modify the installation report once submitted to the municipality?

The installation report is submitted by the Wi-Fi installation company once the installation is complete. By submitting the installation report, the Wi-Fi installation company declares that the installation is complete and compliant with the technical requirements set out in Annex I of the model Grant Agreement. If the installation report has been submitted too fast, the Wi-Fi installation company should ask the municipality to reject it. Provided that the municipality has not yet confirmed the installation report, the installation report will come back to the Wi-Fi installation company for edition.

Once the Wi-Fi installation company has submitted the installation report, the WiFi4EU portal will automatically notify the municipality by e-mail, inviting the municipality to verify the information entered by the Wi-Fi installation company and to confirm that the installation is complete and compliant with the technical requirements set out in Annex I of the model Grant Agreement.

The municipality may reject the installation report. The WiFi4EU portal will automatically notify per e-mail the Wi-Fi installation company and provide the reason for rejection given by the municipality. If the municipality rejects the installation report, it becomes editable for the installation company to modify it and submit it again.

Once validated by the municipality, the installation report is not editable any longer and cannot be modified. In case of changes, the municipality or the Wi-Fi installation company should notify the Executive Agency (via HADEA-CEF-WIFI4EU@ec.europa.eu) who would encode the changes in the WiFi4EU Portal.

The installation report, submitted by the Wi-Fi installation company and approvalby the municipality, is necessary for the Commission to launch its own verifications that the rules set out in the model Grant Agreement are complied with. If all is compliant, the Commission will pay the voucher within 60 days.

6.10 - Can a municipality change its initial choice of the Wi-Fi Installation Company during the implementation period (32 months for Calls 1, 2 and 3, and 24 months for Call 4)?

The Beneficiary (municipality) may change the selection of the Wi-Fi Installation Company. The Beneficiary should ensure that enough time is left within the implementation period (32 months for Call 1, 2 and 3 and 24 months for Call 4) – starting after the countersignature of the Grant Agreement by the Innovation and Networks Executive Agency (INEA) - to complete the installation of the Wi-Fi network(s) by the newly selected Wi-Fi Installation Company. In any case, it should occur before the Beneficiary validates the Installation Report in the Portal (see Q6.7). The Beneficiary can review the Wi-Fi installation company details and update the initial selection on “My voucher” tab, by clicking on the Wi-Fi Installation Company link "See details".

7. WIFI4EU PORTAL

7.1. I cannot log into the WiFi4EU Portal. What should I do?

In case a person no longer has access to the WiFi4EU Portal (i.e. no access to the EU Login credentials used in the original registration), municipalities should contact the Health and Digital Executive Agency (HaDEA) directly via e-mail. Please see the procedure described in Q2.3.

If you are having specific IT/technical issues, please contact the Helpdesk with an explanation of the problem.

8. DATA PROTECTION

8.1. How is my personal data protected?

The WiFi4EU Portal - in accordance with the applicable EU legislation (notably Regulation (EC)2018/1725) only collects personal data necessary for the participation in the WiFi4EU initiative and its management by the European Commission/ the Executive Agency . Data will not be retained unless necessary for control and audit purposes.

Similarly, some of this data may be shared by the European Commission/ the Executive Agency , on the basis of the "need to know" principle, with other EU Institutions and bodies and Member States (including their regional or local authorities), or other services in charge of controls or inspections in accordance with European law (European Court of Auditors, OLAF, Ombudsman, etc.).

For more details, see the WiFi4EU privacy statement, available on the home page of the WiFi4EU Portal.

Please note that for the WiFi4EU network, in Phase I, the registration and authentication of users, and therefore any potential collection and processing personal data, will be the responsibility of each municipality and their contracted Internet Service Provider (ISP). In this phase, each WiFi4EU hotspot will have to comply with a privacy statement and applicable national and EU laws, notably Regulation (EC)2018/1725.

In Phase II, the Single Authentication Service will allow endusers to register only once and "roam" seamlessly between all WiFi4EU hotspots, without having to reintroduce their credentials.

9. TECHNICAL QUESTIONS

9.1. What is the "domain name" as per definition of Article 4.1 of the Grant Agreement?

The domain name is the captive portal web address of the WiFi4EU network (URL). Note that this refers to the website on which the captive portal is located, and not to the website which the user will be redirected after logging in. It is up to the municipality to choose it.

9.2. Access points

9.2.1 What are the technical requirements for the WiFi4EU Access Points?

The technical specifications of the equipment are detailed in section 6.2.2 of the call text, as well as Article I.2 of Annex I of the Grant Agreement signed between the municipalities and the Commission.

The municipality shall ensure that each Access Point:

- Supports concurrent dual-band (2,4Ghz – 5Ghz) use
- Has a support cycle superior to 5 years
- Has a mean time between failure (MTBF) of at least 5 years
- Has a dedicated and centralised single point of management for all APs of each WiFi4EU network
- Supports IEEE 802.1x
- Complies with IEEE 802.11ac Wave I
- Supports IEEE 802.11r
- Supports IEEE 802.11k
- Supports IEEE 802.11v
- Is able to handle at least 50 concurrent users without performance degradation
- Has at least 2x2 multiple-input-multiple-output (MIMO)
- Complies with Hotspot 2.0 (Passpoint Wi-Fi Alliance certification program).

9.2.2. What is the minimum number of Access Points that need to be installed/indoor or outdoor?

The minimum number of Access Points, as also indicated in section 6.2.2 of the call text and Annex 1/Article I.2 of the Grant Agreement, is as follows:

Minimum number of outdoor APs	**Minimum number of indoor APs**
10	0
9	2
8	3
7	5
6	6

5	8
4	9
3	11
2	12
1	14
0	15

9.2.3. Can we reduce the minimum number of Access Points (and at a reduced amount of the voucher)?

No, it is not possible. The number of Access Points is fixed by Annex 1/article I.2 of the Grant Agreement. A derogation on this is not possible because the scheme is not designed to allow partial financing or partial fulfillment of the conditions. However, Access Points may cover several areas even if they are not physically close or interconnected. In addition, more than one Access Point can be installed at a given location (e.g. in order to reinforce the Wi-Fi signal reception).

9.2.4. How many networks should I set up for my project? Is it useful to set up several networks within the same municipality?

One network can host all of the Access Points, irrespective of the internet service provider or the IP of the Access Point. While the creation of multiple networks is allowed in principle, it should be justified by the need to set up and maintain multiple captive portals (one for each network): e.g. one network for the local museum, another network for all of the other Access Points (city hall, pedestrian zone, park, etc.).

As indicated above, although nothing prevents a Wi-Fi installation company to deploy several networks and to split the minimum number of Access Points between different networks, it is highly recommended to deploy as few networks as possible for the following reasons:

1. Networks that include a small number of Access Points are prone to capture only a very small number of connections per week, therefore triggering automatic warning notifications by the WiFi4EU remote monitoring system.

2. Each WiFi4EU network that is deployed has to be connected to a different captive portal.

3. Several networks - and therefore several captive portals - increase the overall operating and maintenance costs.

4. Finally, if there are several networks in operation, the conformity checks performed by the WiFi4EU remote monitoring system before releasing the payment will be done on each declared network separately. In other words, unless each declared network meets the minimum technical requirements as indicated in Article 4.2 of the Grant Agreement (e.g. visual identity, minimum connectivity of end-users), the payment of the voucher cannot be triggered by the Health and Digital Executive Agency .

Nevertheless, it may be useful for a municipality to deploy several networks (i.e. splitting the minimum number of Access Points between several networks) if it considers it essential that its digital services are promoted in separate "landing pages" (captive portal). For example, the municipality may have one network including Access Points located in its city hall/ other public buildings offering eGovernment services to local citizens, as well as another network with Access Points located in the tourist office/other cultural sites, geared for external visitors.

9.2.5. Can I have more than one Access Point at each location?

Yes. The Grant Agreement does not put any restrictions on how the Access Points are distributed. It is purely a decision for the municipalities themselves, taking into consideration how they see the Access Points to best serve the users.

9.2.6. Is the upgrade of existing Access Points covered by the WiFi4EU voucher?

Yes, the WiFi4EU voucher can be used to finance the upgrade of an existing public Wi-Fi network, provided that the upgrade makes the network compliant with the conditions as indicated in the call text (i.e. it respects the WiFi4EU technical requirements). The minimum number of Access Points includes both the installation of new Access Points, as well as the upgrade of existing Access Points.

9.3. SSID (Service Set Identifier)

9.3.1. How should the network (SSID) be set up?

The WiFi4EU network ***SSID*** should be named according to Annex I of the Grant Agreement (article I.5): in particular, the beneficiary shall ensure that the Access Points funded with a WiFi4EU voucher only broadcast "WiFi4EU" as the SSID by default. This SSID name ("WiFi4EU") is therefore information visible to the public, *i.e.* this is the name appearing on the device of any citizen connecting to the hotspot.

The WiFi4EU network ***name*** refers to a name the municipality gives to its WiFi4EU network (e.g. City Hall) to identify it in the WiFi4EU Portal when communicating with the Health and Digital Executive Agency (HaDEA) and to differentiate it from other local networks (when applicable). This information appears in internal reports and it is in principle not disclosed to public.

9.3.2. Can we use an SSID other than WiFi4EU?

In addition to the standard "WiFi4EU" SSID (based on an open network and captive portal), it is possible to also broadcast:

- one SSID for internal use of the municipality, e.g. serving the staff of the administration services in the town hall or in the public library, or for a smart city project.
and/or
- one SSID to provide a secure authentication service of WiFi4EU users in the first phase of the WiFi4EU implementation (e.g. "WiFi4EU – Secure") .

Note that a secured Single Authentication Service serving all WiFi4EU networks in Europe will be established in Phase II of the WiFi4EU implementation (see also Q9.4). Therefore, if a local SSID

providing secure authentication service is established in the first phase (as in the case above), it can either be removed during Phase II or it can continue to be broadcasted in parallel.

In any case, none of the additional SSID broadcasting should affect the quality of service offered to the general public. The municipality should also appropriately differentiate such SSIDs name from the "WiFi4EU" open SSID.

Please refer to the Annex I/article I.5 of the Grant Agreement for more details.

9.3.3. Is the municipality obliged to broadcast an SSID with an open captive portal with no user identification?

The aim of the WiFi4EU initiative is to provide the easiest access possible to free-of-charge Wi-Fi networks in public spaces. We therefore consider that the most straightforward on-boarding procedure, in principle based on a one-click-to-connect button, is preferable. However, should the municipality be required by national laws to put in place other registration and authentication procedures, this can be implemented, e.g. by requesting additional user details. In the absence of such legal obligations, the "one-click-to-connect" procedure should be implemented.

9.4. Who is responsible for the user authentication?

In Phase I of the initiative, the authentication, authorisation and accounting of users is the responsibility of the municipalities. In Phase II, there will be a single authentication system available at EU level, to which municipalities will have to reconfigure their networks to connect to it. The authorisation and accounting of users will continue to be a responsibility of the municipalities. For more details on these two phases, please refer to Annex I of the Grant Agreement.

9.5. Is the "Passpoint" certification required?

As specified in Annex I of the Grant Agreement, a hotspot 2.0 is a requirement for the WiFi4EU equipment to be installed to benefit from a WiFi4EU voucher. The Passpoint Certification Program is required to ensure the interoperability of the equipment not only with other manufacturers, but also with the single authentication service that the Commission will provide at a later stage in Phase II of the WiFi4EU implementation.

9.6. Can you provide a list of equipment that meets the WiFi4EU requirements?

A list of published Wi-Fi CERTIFIED Passpoint® devices can be found by:

- Following the link: https://www.wi-fi.org/product-finder-results
- Choosing the filter ‘Passpoint’, located under ‘Show advanced filters > Access > Passpoint®’.

9.7. Does the WiFi4EU initiative operate a captive portal server?

Annex 1/article I.5.1 of the Grant Agreement lists the requirements to be met for the captive portal in Phase I of the deployment. Note that, there is no centralised captive portal server. In Phase II, the Commission will provide a secured single authentication service and the municipalities will have to

reconfigure their networks to connect to it. Nevertheless, municipalities will need to continue offering the captive portal. See also Q9.4.

9.8. In Phase II of the Wi-Fi implementation, will the secured authentication and monitoring solution require the users to identify themselves in some way (e.g. using a phone number)?

In Phase II, there will be a single registration and authentication system available at EU level that will harmonise the method to on-board users and give them easy access to digital services. At this moment, we do not have additional information on how this will be technically implemented.

9.9. Can traffic on a WiFi4EU network be limited, for instance by setting data or time limits per user to avoid network congestion, or by completely banning access to particular services, contents and sites in order to ensure the security of the network?

Local authorities providing free of charge connectivity to the internet through a local wireless access network under the WiFi4EU Initiative must comply with the obligations to safeguard an open internet access foreseen in Regulation (EU) 2015/2010, irrespective of whether the service is provided through a commercial intermediary or directly by the public local authority.

In principle, as foreseen in article 3, paragraph 1, of Regulation (EU) 2015/2010, providers of internet access services shall treat all traffic equally, when providing internet access services, without discrimination, restriction or interference, and irrespective of the sender and receiver, the content accessed or distributed, the applications or services used or provided or the terminal equipment used.

Limiting data volume per user and/or time limits is allowed as long as the above principles are respected, and subject to the need to ensure a smooth functioning of the network and, in particular, the need to ensure a fair allocation of capacity between users at peak times, according to point I.4 of the Annex I to the Grant Agreement to be signed by municipalities.

Reasonable* traffic management measures are also authorized. In addition, art 3 paragraph 3 foresees the possibility to implement additional traffic management measures justified by the need i.a.:

- To preserve the integrity and security of the network, of services via that network, and of the terminal equipment of end-users.

- To prevent impending network congestion and mitigate the effects of exceptional or temporary network congestion, provided that equivalent categories of traffic are treated equally. More details on how to implement the Regulation can be found in the implementation Guidelines of the Body of European Regulators for Electronic Communications (BEREC).

That been said, in the case of local wireless access networks supported by the WiFi4EU initiative, there is a need to fulfill the applicable eligibility and quality of service requirements: network congestion should not result from the non-respect of the backhaul requirements that guarantee a high-quality internet experience to users (Section I.3).

**In order to be deemed reasonable, such measures shall be transparent, non-discriminatory, and proportionate and based on objectively different quality of service requirements of specific categories of traffic (not on commercial considerations). Such measures shall not monitor the specific content and shall not be maintained for longer than necessary.*

9.10. Is it possible to take a WiFi4EU network out of service during some hours at night?

WiFi4EU networks must offer largely unrestricted access to the Internet, and must be in operation for at least three years from the confirmation of their deployment by the Health and Digital Executive Agency (HaDEA). A remote monitoring system is in place to verify this. Only in case of exceptional circumstances, WiFi4EU networks can be subject to temporary service interruptions. Such interruptions should not last more than the exceptional circumstances that motivated them. The Health and Digital Executive Agency (HaDEA) may request the justification of the exceptional circumstances motivating such a decision.

10. OTHER

10.1. What is the WiFi4EU Community? How can we get involved?

The WiFi4EU Community is an interactive forum that serves as a direct, focal point between stakeholders (i.e. municipalities and Wi-Fi installation companies) for information exchange about the WiFi4EU initiative.

Through blogs, moderated discussions and the sharing of news and information, the Community aims to nurture a dialog and allow participants to share best practices and experiences with each other, as well as enlarge the overall scope of WiFi4EU-related communication.

You are warmly encouraged to join the Community and get involved: https://futurium.ec.europa.eu/en/wifi4eu-community

10.2. What will be the consequences of Brexit for UK applicants?

Please be aware that following the entry into force of the EU-UK Withdrawal Agreement (Agreement on the withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community) on 1 February 2020 and in particular Articles 127(6), 137 and 138, the references to natural or legal persons residing or established in a Member State of the European Union are to be understood as including natural or legal persons residing or established in the United Kingdom. UK residents and entities were therefore eligible to participate in all four WiFi4EU calls.

In addition, UK applicants and beneficiaries remain eligible to receive EU funds for the entire duration of grants implementing the EU's 2014-2020 Multiannual Financial Framework (MFF),

including after the end of the transition period, subject, as always, to compliance with the applicable rules, e.g. on eligible expenditure. This applies to existing grants and ongoing procedures even if the budgetary and/or legal commitment is made after 31 December 2020 on commitment appropriations under the 2014-2020 MFF.

10.3. Is there an "officially certified" WiFi4EU consultant and/or installation company that we should use to help us prepare our application and/or assist us with the implementation?

No. There is absolutely no formal appointment or recommendation of any individual Wi-Fi installation company/consultancy by the European Commission/ Executive Agency under the WiFi4EU initiative. Therefore, please proceed with caution if you have been directly approached and/or have seen advertisements/news items from organisations claiming they are "officially certified" or "officially designated" for this purpose, including by use of WiFi4EU logo and/or the EU flag.

You are also kindly requested to notify and provide these details to the Helpdesk, so that the European Commission can take measures to stop this misinformation. In particular, the European Commission/ Executive Agency reserves the right to withdraw the registration of any Wi-Fi installation company using such uncompetitive practices.

Please note that Wi-Fi installation companies may register on the WiFi4EU Portal at any time. However, the information provided in the Portal by these companies is offered as a reference only. It should not be construed as any formal endorsement of the company/services provided.

It is the responsibility of each municipality to select the Wi-Fi installation company that will set up their WiFi4EU hotspot, in accordance with their standard local procedures (public tendering rules).

10.4. Are there any guidelines available which are applicable to procurement issues affected by COVID-19?

Municipalities and the Wi-Fi installation companies should comply with the national financial rules in terms of invoicing. However, given the circumstances related to the COVID-19 virus, the normal national procurement timelines may be too restrictive, and thus may temporarily inhibit the ability of the contracting authorities to timely react to emergent deadlines, e.g. municipalities wishing to accelerate the award to the Wi-Fi installation company.

There are precedents when exceptional simplification measures were possible in the context of emergency situations.

For instance, in the context of the asylum crisis, the European Commission adopted in 2015 the following guidelines for 'urgent procurements' which gives directions when a direct award would be justified. See https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52015DC0454

National procurement authorities can give advice on the transposition of these guidelines in a national context. See how to contact your national representative at

https://ec.europa.eu/info/policies/public-procurement/support-tools-public-buyers/public-procurement-eu-countries_en

10.5. Will there be an extension of the installation time for WiFi4EU beneficiaries of Call 1, 2, 3 and 4?

The Coronavirus outbreak is severely affecting thousands of municipalities across Europe. We are aware that the strict confinement measures put in place in several European countries are slowing down or even blocking the deployment of WiFi4EU networks. Given these unforeseeable circumstances, the European Commission had first decided to grant an extension of the installation period to WiFi4EU beneficiaries of Calls 1, 2 and 3, of 8 months, and decided later to grant an extension of the installation period to WiFi4EU beneficiaries of all calls of an extra 6 months in order to allow every concerned municipality to complete their projects. The initial 18-month implementation period granted to finalize and declare the installation and operation of the WiFi4EU network extended by an additional 14 month- period for Calls 1, 2 and 3 (32 months in total) and 6 month-period for Call 4 (24 months in total).

10.6. Why is the number of reported connected users / devices by an installation company different from the ones detected by the WiFi4EU monitoring system?

The WiFi4EU monitoring tool can only count the users / devices that have performed the entire connection cycle on the local portal, including the download of the snippet, the proper display of the appropriate WiFi4EU banner on the device and the transmission of snippet data back to the WiFi4EU monitoring servers (which approximately accounts for 70 Kbyte of data transmitted). If the cycle is interrupted, then the WiFi4EU system cannot count the user / device in the statistics. Therefore, all the connections to the access points with less than 70 Kbyte should be automatically discarded from the counting.

10.7. Is one same user counted twice if it reconnects another day?

The WiFi4EU Remote Monitoring System counts the users through the snippet embedded in the captive portal. Therefore, if a user were not shown the captive portal, it would not be counted.

To ensure that daily users are counted, it is recommended to set the “Automatic reconnection” parameter to less than 12 hours.

10.8. Why do I still receive warnings on the non-compliance of the captive portal, if the self-test (self- test modus) results are positive?

Even if the self-test is successfully executed, it does not mean that all users accessing the captive portal will visualize the WiFi4EU logo/banner as it is intended. It only means that the device from which the test was performed was compliant.
Each device used might have different screen sizes sporting different resolutions or configurations to display their contents. The snippet verifies that all of the criteria set in the implementation guide document are met based on that particular device's resolution and/or configuration. This is the reason why the self-test cannot guarantee 100% that the captive portal is working as intended for all the connected devices.

We encourage the installation companies and municipalities to test the snippet implementation on different devices (computers and smartphones, in portrait or landscape mode).

10.9. How should I perform the self-test (self-test modus) described in the installation guide?

The self-Test modus can be activated while developing the local portal. It should be tested on different devices with various screen configurations (small, large, portrait, landscape) in order to validate the proper display of the visual identity. Moreover the test should be done while connecting directly to the WiFi4EU network.

Please note the configuration differences, analyzing the “validation log” and correct the captive portal design accordingly as stated in the instructions of “Snippet installation guidelines” (available herehttps://hadea.ec.europa.eu/system/files/2021-09/cnect-2017-00250-00-11-en-ori-00_0.pdf).
Please pay particular attention to section 5.6 regarding the sizing and positioning of the WiFi4EU visual identity.

Please also ensure that the self-test modus is deactivated after completion in order to secure continuation of the data flow via the snippet to the remote monitoring system of the European Commission/ Executive Agency (“Snippet installation guidelines”, section 6.4).

10.10. Does the snippet in the captive portal collect personal data from the users that connect to a WiFi4EU network?

No. The snippet in the captive portal does not collect any personal data from the users. It only serves to count the number of users of a WiFi4EU network.