Requirement	Arguments	Suggestion
Authentification system	There is no technological necessity for any form of authentification.	Authentification in accordance to national law, even though we doubt any might be in compliance with GDPR.
Authentification system with a two step approach	the two step approach is only nessecary to get time establish the centralized platform	final deployment without centralized authentification
Authentification system first step	Providing a GDPR capable infrastructure at every beneficiary creates costs, allows for monitoring of people working in the building equipped with WiFi4EU	Final authetification system if needed by national law, otherwise no authentification
Authentification system with centralized RADIUS architecture	Personal user information at one central point allows to create travel profiles	No authentification - no personal information
SSID WiFi4EU	We are happy here	SSID WiFi4EU, calrify that a multi SSID use fo the hardware is allowed
Captive portal	Not necessary; excludes various diabled people and unsavy users; disrupts various services	
Registration and authentification of users with applicable national regulation	We doubt that an implementation in comliance with the GDPR are possible	Keep compliance reg. & auth with national regulation if GDRP compliant
Captive portal can establish a period for automatic recognition of previously connected users	This is only possible with the storage of personal information (Mac Address)	No captive portal - not needed;
This period should automatically reset every day at 05:00	This forces the users to log in EVERY day and thus either interrupts the useflow of the device and annoys user or prohibits the use of the wifi4eu network leading to more mobile data use or networks allowing for automatic connection	No captive portal - not needed; given a captive portal still is a bad idea
non IDN captive portal domain	If an captive portal is to be implemented this is necessary	No captive portal -> not needed
https captive portal	https primarily protects the content of a transmission, importent parts of the metadata are not protected. The impact of https to a classic captive portal page view is very limited, if the captive portal is used to enter user credential https is essential.	No captive portal -> drop requierment
Branding the captive portal	Branded captive portals are known to annoy users. A substandard implementation of WiFi4EU might lead to further alienating the european population	No captive portal -> drop requierment
Remote Monitoring	To add remote content to every captive portal page impression allwos to identify the devices via browser fingerprinting. Device blocking remote content via adblocker will falsify the mesurements. Adding active content (JavaScript) from remote sites into an https secured web page blurs security boundaries; in case some malicous party manages to inject malware through this channel, all users of Wifi4EU are at risk.	drop requierment
Radius architecture is required for the registration and authentication	The registration of users need trained personal or the use auf SMS Service or alike. Using a personal registration is expensive and only avaible during office hours. Using SMS registration ist expensive in countries like Germany and discriminates users without a working SIM-Card - the once in the most need for a free WiFi.	Do not use authentification
Branding: The banner will be XXX and the terms and condtions XXX	Branded captive portals are known to annoy users. A substandard implementation of WiFi4EU might lead to further alienating the european population	drop requierment
multible installation sites	The additional effort to allow multible domain names is a result of the plan to add a captive portal.	No captive portal - no exeptions needed
differentiate the authentication requests coming from each APs	This is highly sensitive information, it is even possible to monitore the movements of employees at their workspace.	honor the GDPR, Art. 5 (1) c) limit personal data necessary to the porposes - do not stare any personal data for a free WiFi
Existing networks	Allow the implementaion of WiFi4EU as additional SSID in combination with a VLAN set up	We would need additional time to define a reasonable requierment
At least 9 outdoor access points or 15 indoor access points	In our experience installation of that size cost bring quiet a bit on installation costs. 15.000€ might not be sufficent to cover the entire cost.	Allow for cofinancing by the municaplities
sales cycle superior to 5 years	A guaranteed sales cycle tends to result in higher product price. The manufactures typically provide compatible successor if the original product is no longer avaiable.	stick to recommendation insted of hard limits in such details
a minimum time between failure (MTBF) of at least 5 years	This should be "Mean Time Between Failures", products with high guranteed MTBF tend to be very expensive. In many cases it es more economic to replace some more units.	stick to recommendation insted of hard limits in such details
configure all the APs installed from a single point	This is really important, espacially to be able to easyly provide software updates	keep this requirement
comply with the 802.11ac Wave I	This is a good compromise between price and performance, most vendors are able to deliver these products	keep this requirement
support 802.11[x] IEEE	This is redundant to "comply with the 802.11ac Wave I", and might be misinterpret as 802.1 x	drop this requirement
Each AP will be able to support at least 3 different service set identifiers (SSIDs)	We agree	keep this requirement
handle at least 50 concurrent users without performance degradation	That needs clerification, since the wireless bandwith is a shared medium it is only possible to provide the maximum bandwith to one device. The important point is that the AP is able to maintain its overall bandwith with a certain number of clients.	Require the APs to handle a stable overall throuput with 50 users
have at least 2x2 MIMO	2x2:2 is a real minimum for 802.11ac. Higher numers of sparcial streams having a strong impact of the necessary airtime. This has a great potential to improve performance in high density areas like city centres	Demand 2x2:2 MIMO while recommending 3x3:3
comply with Hotspot 2.0	This is only a fix for some problems resulting from the introduction of an authenification system. The benefit of a Hotspot 2.0 System is the transparent login to the WiFi without the need to log into the captive portal. This is a build in feature of any open WiFi without a captive portal. Additionaly making the Hotspot 2.0 functionallity a requierment could be seen as economic favoritism towards apple products.	No captive portal - no need for Hotspot 2.0
	In order to allow the construction of mesh networks necessary to for uninterrupted roaming use including the IEEE 802.11s standard is a necessisty	Require IEEE 802.11s compability for new installments

subscription to the highest available mass-market offer; at least 30 Mbps	If meshing protocolls are included this might lead to unfittign of internet access, we recommend a ratio of 0,5 mps bandwith per outdoor user.	keep requierment
The backhaul speed should also be at least equivalent to that		keep requierment
The Commission will remotley monitor the quality of the connectivity	So far we see no technical viable option to do so, we like the problem.	technically not a requierment
	Given that open source software has a much stronger track record with regards to IT Security, recommend the use of open source software. Doing so should also save funds throughout in the entire project. Pleas talkt to the Free Software Foundation about the advantages of using open source software in public service.	recommend use of open source implementations