Grant Agreement No.: 732638
Call: H2020-ICT-2016-2017
Topic: ICT-13-2016
Type of action: RIA


# D2.05: End-User Validation

| | |
|---|---|
| Work package | WP 2 |
| Task | Task 2.8 |
| Due date | 31/10/2017 |
| Submission date | 08/03/2018 |
| Deliverable lead | Mandat International |
| Version | 1.0 |
| Authors | Christopher Hemmens (MI), Adrian Quesada Rodriguez (MI), Cédric Crettaz (MI), Sébastien Ziegler (MI), |
| Reviewers | Maria Chiara Campodonico (Martel) |

| | |
|---|---|
| Abstract | This deliverable presents the methodology to be applied during the end-user validation in the context of Fed4FIRE+. This document describes the legal requirements, in particular the GDPR, what Fed4FIRE+ must comply. |
| Keywords | End-user, GDPR, personal data protection, methodology, validation |

### Document Revision History

| Version | Date | Description of change | List of contributor(s) |
|---|---|---|---|
| V0.1 | 31/08/2017 | TOC | C Hemmens (MI), S Ziegler (MI) |
| V0.2 | 09/10/2017 | 1st Draft | C Hemmens (MI), A Quesada Rodriguez (MI), C Crettaz (MI), S Ziegler (MI), B Vermeulen (UG), D Margery (INRIA), J Iranzo Yuste (ATOS) |
| V0.3 | 18/10/2017 | 2nd Draft | C Hemmens (MI), S Ziegler (MI), A Quesada Rodriguez (MI), C Crettaz (MI) |
| V0.4 | 26/10/2017 | Deliverable review | M.C.Campodonico (Martel) |
| V1.0 | 30/10/2017 | Addressed comments in review | C Hemmens (MI) |

## DISCLAIMER



## COPYRIGHT NOTICE



## ACKNOWLEDGMENT

Co-funded by the European Union

Co-funded by the Swiss Confederation

This deliverable has been written in the context of a Horizon 2020 European research project, which is co-funded by the European Commission and the Swiss State Secretariat for Education, Research and Innovation. The opinions expressed and arguments employed do not engage the supporting parties.

| Project co-funded by the European Commission in the H2020 Programme | | |
|---|---|---|
| **Nature of the deliverable:** | | **R** |
| **Dissemination Level** | | |
| **PU** | Public, fully open, e.g. web | ✓ |
| **CL** | Classified, information as referred to in Commission Decision 2001/844/EC | |
| **CO** | Confidential to FED4FIRE+ project and Commission Services | |

** R: Document, report (excluding the periodic and final reports)*

*DEM: Demonstrator, pilot, prototype, plan designs*

*DEC: Websites, patents filing, press & media actions, videos, etc.*

*OTHER: Software, technical diagram, etc.*



Co-funded by the Horizon 2020 Framework Programme of the European Union

# EXECUTIVE SUMMARY

This deliverable sets out a methodology for conducting end-user validation for the Fed4FIRE+ service. It outlines the questions that need to be asked, to whom, and in what form. It also determines how the data elicited from end-users will be stored, what the legal requirements of the project are on personal data protection, how the data will be processed and analysed, and what results are most relevant to the Fed4FIRE+ service.



Co-funded by the Horizon 2020
Framework Programme of the European Union

# TABLE OF CONTENTS





Co-funded by the Horizon 2020
Framework Programme of the European Union

Co-funded by the Horizon 2020
Framework Programme of the European Union

# LIST OF FIGURES





Co-funded by the Horizon 2020
Framework Programme of the European Union

# ABBREVIATIONS

| | |
|---|---|
| **DPO** | Data Protection Officer |
| **EU** | European Union |
| **FIRE** | Future Internet Research and Experimentation |
| **GDPR** | General Data Protection Regulation |
| **IoT** | Internet of Things |
| **PbD** | Privacy by Design |
| **PDP** | Personal Data Protection |
| **PII** | Personally Identifiable Information |
| **R&D** | Research and Development |
| **SLA** | Service-Level Agreement |
| **SME** | Small-to-Medium-Sized Enterprise |
| **TaaS** | Testbed as a Service |



Co-funded by the Horizon 2020
Framework Programme of the European Union

# 1. INTRODUCTION

Fed4FIRE+ is the direct successor of the Fed4FIRE project that ran from 2013 to 2016. It was developed at the same time as other federation projects such as XIFI, IoT Lab, and OneLab and was chosen to be further developed due to its popularity and status as the key reference point for the FIRE (Future Internet Research and Experimentation) community.

As Fed4FIRE+ is built upon the work of Fed4FIRE, there is no set-up phase and, therefore, the project started accepting submissions from launch.

## 1.1 OBJECTIVES

Fed4FIRE+'s primary objective is to build upon and improve the infrastructure already put in place during the development of Fed4FIRE. This will include exploiting and expanding the existing facilities, upgrading and improving them, and extending their functionality to the wider community and marketplace.

Following dedicated market analysis, the federation is focussed on fixed and wireless infrastructure, services, and applications in relation to cloud computing, big data analysis, media delivery networks, smart cities, 5G, and IoT. New facilities can join at any time conditional on their ability to meet a set of entry requirements that may be updated over time.

The project will, ideally, ultimately serve as a streamliner for people and other research entities to use testbeds across the world and allow them to conduct experiments at a fraction of the cost and over a shortened period of time. An expected consequence of this is that Fed4FIRE+ will permit research that will set new standards for scale and influence and significantly increase the speed of scientific progress and reduce costs in the decades to come.

## 1.2 VALUE PROPOSITION

As laid out in the Description of Action, here are the main reasons to participate in Fed4FIRE+:

For experimenters

1. Easy access to a wide variety of testbed facilities
2. Low- or zero-cost access to testbed facilities
3. Option of using multiple testbeds in a single experiment
4. Access to newly-launched testbeds
5. A single portal for all testbeds
6. Additional tools to help manage experiments running on multiple testbeds
7. Support for experimenters



Co-funded by the Horizon 2020 Framework Programme of the European Union

For testbed providers

1. Access to a large group of experimenters
2. Greater chance of success stories potentially attracting additional funding
3. Greater diversity of potential experimenters from different application domains
4. Possibility of gaining enhanced functionality through services provided by Fed4FIRE+
5. Increase its own visibility
6. Become part of a large community of researchers and testbeds
7. Become a member of the de facto premier European FIRE federation

## 1.3 CONCEPT

The original Fed4FIRE project found a way of connecting lots of disparate unconnected testbeds covering a huge range of sizes, locations, and purposes. By building an infrastructure that would allow access to all of them as if the user were using each testbed directly as well as making the interface simple enough that any experimenter could conduct their experiments without any detailed understanding of the way the service they were using operated, Fed4FIRE created an invaluable tool for 21st-century research and business support. Fed4FIRE+ continues to improve the service and and create new and innovative tools that will help support an already successful project.

In addition, Fed4FIRE+ will build upon the following projects:

- OpenLab: experimental plane middleware facilitating the use of the testbeds;
- CREW: a federated test-platform using advanced spectrum-sensing, cognitive radio, and cognitive networking strategies;
- WiSHFUL: software for controlling the radio and network aspects of different devices;
- IoT Lab: crowd-sourcing and crowd-sensing technology for ICT research;
- F-Interop: online testing tools including interoperability, conformance, and performance-testing;
- FORGE: a program looking to bring FIRE technology to eLearning such as Open Educational Resources, MOOCs, and eBooks;
- and SUNRISE, MONROE, GEANT, FUTEBOL, and TRIANGLE among others.

Eventually, Fed4FIRE+ will create an open marketplace for experimenters which will simultaneously allow the project to become self-sufficient and generate data on stakeholders' needs. Open Calls will also be initiated to allow external entities to develop and improve the network.



Co-funded by the Horizon 2020 Framework Programme of the European Union

Importantly, there will be a renewed focus on:

- personal data protection in line with the European Parliament's General Data Protection Regulation (GDPR),
- the reuse of data generated by the project in participation with the H2020 Pilot on Open Research Data,
- building trusted relationships across the network modelled on the Federated Trust and User Experience framework,
- facilitating replicability of experiments' results,
- building a robust authentication service upon the prototype authentication proxy of Fed4FIRE to ease the introduction of new experimenters and testbeds,
- improving the legibility of descriptions covering every aspect of the federated process allowing, for example, easier discovery of resources and services, the application of optimal infrastructure, and the ability to monitor the usage and availability of billing and SLA checks.

## 1.4 WORK PACKAGE 2 - FEDERATOR

This Work Package is dedicated to running and administering the federation. Its primary goals are to ensure that the following tasks are taken care of: operations, management, control, improvements, requirements, and sustainability. This is such that the testbeds are maintained and remain well-connected to the larger system.

To do this, the Work Package will define and implement the mechanisms that will determine how the testbeds and federation at large are monitored, accessed, combined, and improved. This is a continuation of the work already completed in Fed4FIRE and other former FIRE projects.

The basic funding for the project is also included in this Work Package alongside that for the open calls on testbed and tool extensions.

## 1.5 TASK 2.8 - END-USER VALIDATION

Task 2.8 is responsible for getting feedback from users of the Fed4FIRE+ service predominantly through open calls. This forms part of the "Experiment Cycle" in which users use the service, provide feedback to the federator, the federator evaluates the feedback, and finally the federator updates the service in line with the feedback received. This happens multiple times with the purpose of ensuring that the federation service is of optimal quality.

The feedback elicited will focus on the testbeds and tools used and, in particular, users' experiences of using them and their impact on the users' businesses.



Co-funded by the Horizon 2020 Framework Programme of the European Union

## 1.6 DELIVERABLE 2.5 - END-USER VALIDATION

This deliverable is the first of three (followed by D2.10 in M30 and D2.14 in M60) all focussed on the collection of feedback from users and overall improvement of the Fed4FIRE+ service. The objective of the deliverable is to set out a methodology for conducting the end-user validation which will then feed into the general improvement of the Fed4FIRE+ service.

It starts by answering the following questions:

- From whom will we get feedback?
- About what will we get feedback?
- In what form will this feedback be?
- How will we request the feedback?
- Must the data be anonymised before use?
- How would we do that?
- How will we analyse the data?
- What results are most important for validation?

This list includes a first set of questions and it is expected to be expanded in future iterations.

After doing that, these answers will be combined into a cohesive whole that will form a comprehensive roadmap for Task 2.8 as well as other parts of Work Packages 2 and 5.

The deliverable also includes a detailed breakdown of the privacy guidelines in relation to the European regulations on data protection that we must adhere to in the process of end-user validation.



Co-funded by the Horizon 2020
Framework Programme of the European Union

# 2. METHODOLOGY

## 2.1 WHAT IS END-USER ENGAGEMENT?

End-user engagement refers to the inclusion of people who will ultimately use the service in the design of the service itself. Not only is there many ways of doing this, but also lots of different types of engagement too. For example, one aspect could be simply the provision of information - a website containing detailed information about the service or what the aims and goals of the service are, who the intended users are, and where it fits the wider research ecosystem.

There are more direct forms of engagement including surveys and crowdsourcing that gain opinions and suggestions from the people using the service allowing the designers to improve it in a much more efficient and incisive way then keeping the whole feedback process constrained to the design team.

Both of these approaches serve to enforce a connection between the designers and users that is useful beyond simply getting feedback or informing the public; by creating that connection, it's possible to build new marketing opportunities and gain access to complementary projects that may be combined with to form stronger and more beneficial alliances.

## 2.2 METHODOLOGY

End-user validation falls within the Experiment Cycle seen here alongside the Innovation Cycle and Business Cycle.

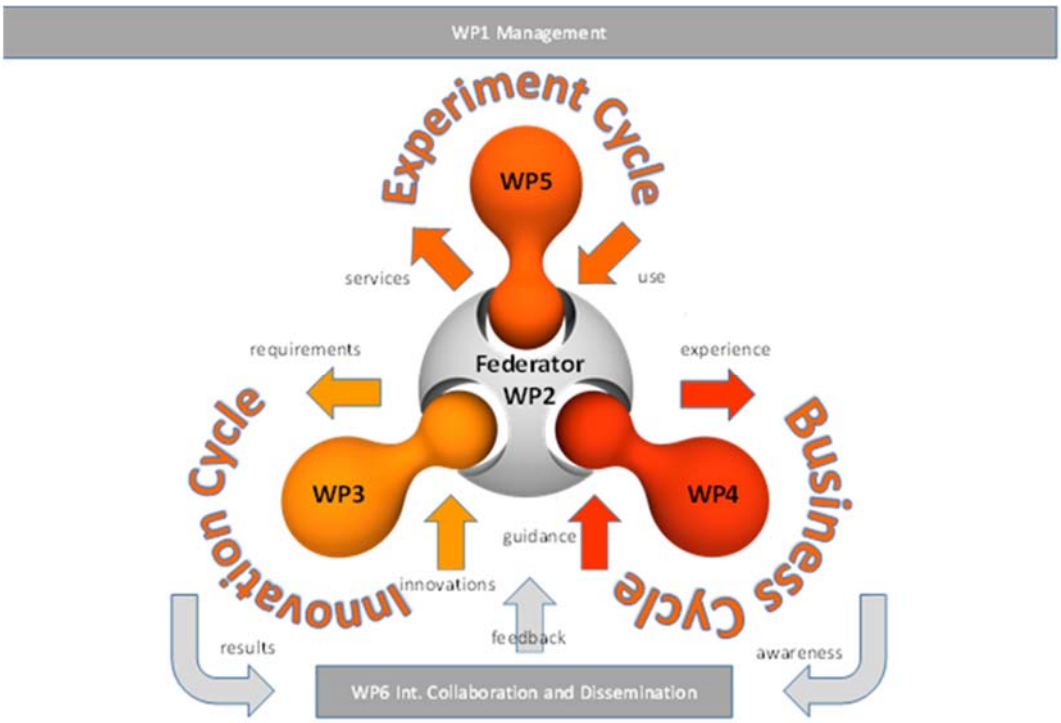


Figure 1. Set-up of the Fed4FIRE+ Project



Co-funded by the Horizon 2020 Framework Programme of the European Union

The Experiment Cycle can be described following these steps:

1. The Federator operates the service
2. The Users use the service via open calls
3. The Users identify problems or potential improvements in the service
4. The Federator collects feedback from the users
5. The Federator evaluates the feedback
6. The Federator fixes the problems, implements the improvements, or issues an new open calls related to the feedback (WP5).
7. Go to step 1.

The task of validation covers steps 4 and 5 in this cycle although it needs to coordinate carefully with the other steps to make sure the cycle runs smoothly and efficiently.

The Cycle also covers Work Package 5 in addition to Work Package 2 as WP5 is responsible for issuing Open Calls on behalf of the federation. Any feedback that the federation receives as part of the validation process can be sent to this Work Package group so that they will be informed on what issues they need to focus on.

Validation starts by identifying the different categories of user that we expect to have using the service. These will generally be people or groups who are engaged in conducting research or testing and so will normally come from R&D and related sectors, whether they are for publicly- or privately-funded institutions. There may be other users who do not fall into these categories, however, the former are likely to be the core of our user base.

The survey detailed below will be implemented using the Lime Survey tool run by Mandat International as part of IoT Lab. Registered users of Fed4FIRE+ will be sent links to the survey either directly on the website or via the crowdsourcing tool, also provided by Mandat International. The survey will collect data about the projects that the users are working on, what parts of the Fed4FIRE+ service they used, what they think of the service, what they think of the open calls (if they participated in them), what they think it should be improved, and, finally, questions about their understanding of privacy and data protection standards in relation to the service.

In addition to the survey, the federator will collect metadata from the various projects registered on the Fed4FIRE+ service looking primarily at tools and testbeds used, duration of use, location data, and more. Some of this will be used to directly evaluate the way the Fed4FIRE+ service is being used, however, the federator will also use it to analyse how the respondents to the survey compare to the overall user base and this will inform our evaluation of the survey feedback. If, for example, a lot of survey respondents call for a particular change but there is a certain type of user who is both unlikely to respond to the survey and likely to be negatively impacted the change, the metadata will help the federator to decide whether to implement the feedback that comes through in the survey.

In line with European privacy regulations, all data collected by Task 2.8 will either be pseudonymised or fully anonymised. This will protect the users from misuse of data while ensuring that we get optimal results from the data analysis.



Co-funded by the Horizon 2020
Framework Programme of the European Union

Finally, the federator will collate all of the suggestions raised in the surveys, generate the dataset based on satisfaction ratings by users, and compile the data sets on testbed and tool usage, geographical and sector popularity, and impact on users' projects. By performing analyses on these three types of feedback, we will generate a set of recommendations that will be used to improve the Fed4FIRE+ service. This will be followed by another round of user feedback solicitation later in the project.

## 2.3 CATEGORIES OF END-USER

Fed4FIRE+ is suitable for people across different target groups including academia, industry, and SMEs. All of them will use the service in different ways and a crucial part of validation is that all intended users are satisfied with the service they receive.

### 2.3.1 Academics

Academics are most likely to be based at universities but may also work from home or in the capacity of a tutor to others. Their working situations are likely to be more idiosyncratic than those working in industry or for a company due to the nature of the work they are conducting. For this reason, it's important that the service is flexible and can fit into as wide range as possible.

### 2.3.2 Industry

People working in industry are likely to be highly goal-focussed and will therefore require a service that works quickly and efficiently. To this end, it's important that the service is clear and well-structured and that delays in results are minimal.

### 2.3.3 SMEs

Similar to people working in industry, SMEs are also highly goal-oriented, however, their resources are likely to be more limited and will theoretically looking for the maximum amount of output for a relatively small amount of input. These people will be looking at minimising false moves and working within not only a financial budget but also a time budget. This requires the service with the largest amount of information possible in the shortest time.

## 2.4 DATA COLLECTION

Before the validation takes place, the data must be collected. This will be done using both direct and indirect means. In all cases, data will either be anonymised or pseudonymised so that no individuals can be identified from the inputted data. This is important for meeting the obligations to data privacy protection regulations.

Directly, surveys will be sent to users using LimeSurvey and gather 'soft data' regarding their experiences and opinions about how the service is working and what could be done to improve it. Users will be reminded that Fed4FIRE+ is continuously under development and that every response will help improve it.

User data provided in the survey responses will be matched against the user profiles received upon registration with the service to ensure that the survey responses are as representative of the user population as possible. Discrepancies in survey respondents and the user population will be reported and remedies for improving survey participation will be constructed. This process involves only matching of the demographic make-up of the different samples and no point looks at individual profiles.



Co-funded by the Horizon 2020 Framework Programme of the European Union

Indirectly, the data gathered will concern:

1. the cross-section of testbeds being used,
2. what they are being used for,
3. for how long,
4. at what times they're being used,
5. what the change in use for each testbed is over time,
6. plus other 'hard data' to be considered.

## 2.5 ANALYSIS

Much of the survey data will come in the form of opinions and will therefore need to be transcribed into a more analysable form. Since we cannot predict in advance what the answers will be, the most productive method for analysing the suggestions will be to go through every response and generate short summaries that can either be put into an existing category of response or form the basis of a new category. Theoretically, this process should only be necessary for the first round of surveys as subsequent surveys will be able to employ these categories in the form of drop-down menus.

This first set of data will outline direct calls for improvement in the service which will be addressed one-by-one. The satisfaction data, on the other hand, will need to be distilled into a numerical dataset with answers being tied to user demographics as well as testbed and tool statistics. Using standard statistical techniques, it will be possible gain an overall impression of how satisfied users are of the service as well as the individual tools. In general, a satisfaction rating of 4.0 will be deemed satisfactory (based on 1-5 scale where 5 is the highest level of satisfaction).

The final dataset, which will be analysed using a mixture of statistical and more scrutinised analysis, will be comprised of the metadata including general location, duration, and general testbed used data. This dataset will determine if the service is being used in the way we intended it to be employed, which will then tell us if we need to:

1. focus our dissemination and marketing at different things,
2. change what we think the service is primarily for and alter our innovation efforts, or
3. continue the current strategy for innovation and dissemination.

The combination of all three results above will lead to a set of recommendations for improving the service as well as maximising aggregate satisfaction among all end-users including researchers, testbed operators, and more.



Co-funded by the Horizon 2020 Framework Programme of the European Union

# 3. END-USER VALIDATION TOOLS

## 3.1 OBJECTIVES

The purpose of the end-user validation is to identify opportunities for improvement in the service. These opportunities can either be related to the technical part of the service (the backend), the user experience (the frontend) or other issues such as those to do with administration or documentation. In addition, many of these issues can either be related to functional aspects of the service that affect the usability of the service or the aesthetic aspects, the latter is less about usability and more about how the service feels to use including some perspectives as at least as important as functionality.

Validation will be broken down into several sections:

1. Impact assessment for end-users
2. User satisfaction
3. Identification of areas for improvement
4. Identification of means of end-user outreach and engagement

The first section is the most straightforward and comprises the initial questions in the survey. This is intended to get users in the mood for answering questions. This segues smoothly into the questions relating to user satisfaction and identification of areas for improvement which will ultimately be the main focus for the validation activities.

## 3.2 SURVEY

The primary source of end-user feedback will come in the form of a survey. This section presents an initial draft of that survey which can be sent to users at key moments in the evaluation process.

The survey consists of 26 questions.

### User project

*The survey starts by asking the user about the project they're working on. These are straightforward questions that identify the type of user as well as easing them into the survey whose questions begin to require more thought later on. This information will later be cross-checked with the metadata to see who is more likely to respond to our calls for feedback and where we can improve our communication with end-users.*

1. What is the name of your group/project?
2. In which country is your project primarily based?
3. Please describe your project/experiment. (For example, whom is it aimed at? What problems does it attempt to solve?)
4. What is the duration of your project/experiment? (For how long did you use the Fed4FIRE+ service?)



Co-funded by the Horizon 2020 Framework Programme of the European Union

5. What is the application domain of your project/experiment? (For example, smart cities, smart offices, etc.) Choose from: Academia, SME, Industry, Other.

## Fed4FIRE+

*These questions relate directly to the user's perception of the service, which parts of it they used (this information will also be cross-checked with the metadata for the same reason as highlighted above), what they think is missing from the service, and solicits information about potential channels of communication that could be useful for the service. This information will also be shared with the partners in Work Package 5 so that they can use it for generating and evaluating their work in the Open Calls.*

1. How did you find out about Fed4FIRE+?
2. Which testbed/tool(s) did you use?
3. Which aspects of your previous answer did you primarily use for your project?
4. How would you rate the satisfaction with the service? (5-point scale for the following)

4.1. Fed4FIRE+ website

4.2. Ease of access to the service

4.3. Support from Fed4FIRE+

4.4. Results relative to expectations

4.5. Contribution to your project

4.6. Technical capabilities

5. In your opinion, what are the best three features of Fed4FIRE+ in any order?
6. In your opinion, what are the three features of Fed4FIRE+ that need the most improvement?
7. Please provide additional comments if you have any.
8. Did you use the tutorials or demos on the website?
9. Did you participate in any of the Open Calls?
10. How would you rate your satisfaction with the Open Calls? (5-point scale)
11. Please provide additional comments if you have any about the Open Calls.
12. How likely are you to recommend Fed4FIRE+ to colleagues? (5-point scale)
13. Whom should we inform about Fed4FIRE+'s capabilities? (These can include email addresses, websites, etc.)



Co-funded by the Horizon 2020 Framework Programme of the European Union

### Future

*This remains an extension of the previous section but frames it in such a way that encourages users to be more imaginative and positive with their answers.*

1. How likely are you to use the service again or would you recommend the service to others? (5-point scale for the following)

1.1. Willingness to use again

1.2. Would recommend to others (industry)

1.3. Would recommend to others (academia)

2. What improvements would you like to see in the service?

### Privacy

*Due to the focus on personal data protection and privacy by the European Commission, these questions will help us to see how users perceive this dimension of their online work and help not just the Fed4FIRE+ project, but also highly relevant and interconnected projects that Fed4FIRE+ collaborates with.*

1. Do you think you have received sufficient information regarding the way in which your experiment addresses privacy and personal data protection?

2. Are you aware of any privacy or security risks, any vulnerability or something else that you think should be addressed in the Fed4FIRE+ platform?

## 3.3 SOLICITING RESPONSES

The survey will be distributed through the crowdsourcing application developed by Mandat International as part of IoT Lab available for Android and iOS smartphones. Since the app connects to the survey directly through the IoT Lab website, the survey is also available through web browsers and all of the results are collected in a single repository.

Users will be emailed with a link that either connects them to the survey or allows them to download the crowdsourcing app. It is expected that most users will complete the survey through the browser; however, the appeal of the smartphone app is that it can collect a variety of other data including movement, light sources, and temperature. We currently have no use for these features, however, the possibility is there should we find the opportunity arises.

A reminder to complete the survey will be sent and if the number of responses to the survey is low after the reminder, it should be discussed whether additional incentives to encourage users to complete the survey should be introduced.



Co-funded by the Horizon 2020 Framework Programme of the European Union

## 3.4 HARD DATA

Due to privacy concerns, the amount of 'hard data' Fed4FIRE+ can get directly from its users is limited to the number of users, their geographical spread and the companies that are involved including their size, location, sector and whether they are in research or industry. This is useful in and of itself because it will allow us to evaluate the reach and visibility of the network beyond the 'soft data' provided by the survey as well as context regarding the kinds of users we're reaching and what they're likely to be using the service for.

By following the spread of registrations, we can determine if the service is becoming more or less popular and, indeed, by combining this with the survey results, we can determine why it's gaining popularity in some areas and not in others.

In addition to the data Fed4FIRE+ can directly access, it is possible to get them directly from testbeds, although this increases the complexity of ensuring user privacy and should only be done if it is deemed to be strictly necessary. For example, IMEC (formerly known as iMinds) runs one of three Fed4FIRE+ authorities and alone controls the metadata for 99% of Fed4FIRE+ users.[1] This metadata includes names, companies, locations, and the resources they've asked to use as well as descriptions of the projects they're working on.

In addition to this, IMEC runs the jFed tool which allows researchers to keep all their resources and settings logged in a central authority reducing the time required to recover prior experiments.

### 3.4.1 How to use the metadata

Clearly this metadata cannot be used as it is because it would breach the data protection regulations of the EU. Indeed, there is no need to collect data such as individuals' names. It suffices to list the data required for user validation, which are:

- Company research/industry sector
- Company size (people and/or market capitalisation)
- Company location
- Duration of project
- Scale of project
- Whether the user is returning to the service or not

and in a separate list:

- Types of resources requested
- Scale of resources requested
- Times of use e.g. night, day, etc.

[1] The other authorities are PlanetLab Europe and Fed4FIRE Portal.



Co-funded by the Horizon 2020 Framework Programme of the European Union

- Testbeds requested

The reason for keeping separate lists is that, by cross-correlating the two lists, it is possible to gain all of the required information for validation while simultaneously pseudonymising the data. This means that it is possible to run a full analysis of the data and protect data privacy at the same time.

In order to facilitate this, the Fed4FIRE+ terms and conditions that all users agree to when they start using the service will be updated to contain a clause stating that their data will be used for user validation or equivalent. Until this clause has been added and users have been given reasonable warning that this change has been made, it is not permitted to use the data listed above in the manner outlined.

An email detailing the changes will be sent out to all registered users and the option to not have their data used will be given. It will be made clear, in any case, that even if the usage of personal data, it will be fully pseudonymised in accord with the EU's privacy regulations.

As an additional measure, each testbed will be asked to designate a Data Protection Officer (Testbed DPO) who will coordinate with the Project DPO for Fed4FIRE+ in ensuring the security of the data they hold, as detailed in the section on Personal Data Protection found below.

In addition, it is important to emphasise that, in line with European regulations, personal data cannot be sent outside of Europe if the competence of GDPR is not also applied by the organisations based outside the EU. There has been some discussion surrounding the combination of Fed4FIRE+ with other federations, testbeds and other related research projects outside of Europe. The easiest solution to this problem would be to change the terms and conditions to prohibit the processing of personal data. This would result in the only personal data the federation receives coming from outside the EU, which, even then, would only be for authentication and identification purposes. This would need to be coordinated with the federation once DPOs have been selected for every testbed in the federation.



Co-funded by the Horizon 2020
Framework Programme of the European Union

# 4. PERSONAL DATA PROTECTION POLICY, STRATEGY AND METHODOLOGY

## 4.1 PERSONAL DATA PROTECTION POLICY

The protection of personal data is a topic of especial relevance in the European context, where it has long been introduced into numerous normative frameworks[2].In its efforts to protect the fundamental rights and freedoms of natural persons with regard to the processing of personal data, the General Data Protection Regulation (GDPR)[3] establishes the following fundamental principles:

- **Lawfulness**: processing takes place in the context of express consent by the data subject (or one of the necessity scenarios found in Article 6 of the GDPR)
- **Fairness**: processing accounts for the need for protecting children and other vulnerable individuals.
- **Transparency**: any information and communication relating to the processing of personal data should be easily accessible, easy to understand and that clear and plain language is used.
- **Purpose limitation**: personally Identifiable Information (PII) should be collected for specified, explicit and legitimate purposes and not subjected to further processing incompatible with those purposes.
- **Data minimisation**: collected data is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- **Accuracy**: data are kept up to date and reasonable steps are taken to ensure the erasure or rectification of inaccurate data.
- **Storage limitation**: data are only stored in manners which permit the identification of data subjects for the minimum necessary timeframes to perform the purposes of collection/processing. (Longer periods are sometimes possible according to Article 5 of the GDPR).
- **Integrity**: technical and organisational measures are implemented to prevent unauthorised or accidental modification and erasure of PII.
- **Confidentiality**: technical and organisational measures are implemented to prevent unauthorised or accidental access and disclosure of PII.

[2] Normative dispositions regarding or related to Personal Data Protection can be found in: The European Convention on Human Rights (Art. 8); the Charter of Fundamental Rights of the European Union (Article 7); the Council of Europe's Convention 108 for the protection of Individuals with regard to Automatic Processing of Personal Data (Art. 1); the Treaty on the Functioning of the European Union (article 16); Regulation 45/2001/EC on the protection of individuals with regard to the processing of personal data by Community institutions and bodies and on the free movement of such data; the Data Protection Directive 95/46/EC); the Privacy and Electronic Communications Directive 2002/58/EC, as amended by Directive 2009/136/EC; and more recently the GDPR.

[3] European Parliament and European Council, "Regulation (EU) 2016/679 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)," accessed January 9, 2017, http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf.



Co-funded by the Horizon 2020 Framework Programme of the European Union

- **Accountability**: compliance with these principles, and in general with the normative framework that surrounds personal data is the responsibility of the controller, as is the burden to demonstrate compliance.

These guiding principles apply whenever Personally Identifiable Information (PII) is compiled, stored, processed, disclosed or otherwise handled, and should be considered by all End-user validation activities taking place in the framework of Fed4FIRE+. In addition to these principles, it is important to remember that the GDRP includes specific dispositions (Art. 25 of the GDPR) to include the principles of privacy by design and by default (hereinafter "PbD") to the European Normative Framework for Personal Data Protection, a concept which rests on seven foundational principles, namely:

1) **Proactive not reactive**; preventative not remedial: the PbD approach aims to anticipate and prevent privacy invasive events (and possible affectations to the rights of data subjects) instead of reacting (and trying to remediate) them.

2) **Privacy as the default setting**: privacy enhancing settings and technologies are enabled by default, not requiring further intervention by the end-user, thus ensuring their automatic protection from privacy invasive events.

3) **Privacy embedded into design**: privacy considerations come as a fundamental pillar to be considered and supported throughout the design of any process or system and not as an afterthought.

4) **Full Functionality – positive-sum, not zero-sum**: the perspective considers that it's possible to find a balance between all legitimate interests and objectives, and to enhance the functionality of the system without introducing any drawbacks.

5) **End-to-end security – full lifecycle protection**: personal data is protected by the approach even before collection, and continues doing so through the collection, processing and deletion processes through the adoption of strong technical and organisational security measures.

6) **Visibility and transparency – keep it open**: the approach aims to generate and enhance user trust in the system/business/process through enhanced transparency mechanism and openness to all interested parties.

7) **Respect for user privacy**: the interests of data subjects are of paramount importance to this approach, as is enabling the participation and empowerment of end-users in the determination and control over the processing of their data.

As detailed in Article 25 and Recital 78 of the GDPR, Privacy by Design and by Default can be enabled by the adoption of measures aimed to minimise the processing of personal data, pseudonymising personal data as soon as possible, enabling the data subject to monitor the data processing, ensuring that by default only the necessary personal data are processed, and preventing the disclosure of PII to an indefinite number of natural persons. A final set of related dispositions can be identified in the ePrivacy Directive[4], which declares not only the prohibition of intercepting the communications (Art. 5) of users of a public communications network or publicly available electronic communications service, but also the necessity to protect (erase or make anonymous) both transit (Art. 6) and localisation (Art. 9) data.

[4] European Parliament and European Council, "Directive 2002/58/EC (as Amended by Directive 2009/136/EC) Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications" (2009).



Co-funded by the Horizon 2020 Framework Programme of the European Union

Given this context, Fed4FIRE+ testbeds are not only obliged to adopt a perspective which ensures the respect for the principles and responsibilities detailed throughout the relevant legal framework, but also to integrate the necessary technical and organisational privacy and security safeguards (included but not limited to strong pseudonymisation, anonymisation and encryption mechanisms) into the design of every single process which could potentially relate or generate PII, including end-user validation techniques.

Considering the nature of the hard data available to the Fed4FIRE+ testbed owners (as detailed in previous sections), and particularly the fact that processing any kind of personal data is not amongst the objectives of the project, the system's processes shall be based fundamentally in the prevention of any possible affectation to the privacy of data subjects through the implementation of the Privacy by Design and by Default principles. Particularly, the system shall introduce strong transparency and information policies at all levels of the Federation (with special focus to inform testbed owners, experiment owners and end-users), aimed at ensuring informed consent to the Platform's Terms and Conditions as necessary to the execution of user authentication and identification by the Fed4FIRE+ systems. Finally, the system shall ensure that the general performance metrics or any other system report which might be published or disseminated to third parties are generated upon anonymised or pseudonymised data, to minimise the possibility of exposing PII (or the data subjects) to risk.

## 4.2 PERSONAL DATA PROTECTION STRATEGY

The personal data protection strategy for Fed4FIRE+ end-user validation is to be implemented on two main fronts, namely:

a) A layered strategic approach to PDP will aim to ensure the greatest possible level of compliance with both the GDPR and local (or sector-specific) primary (and secondary) legal requirements. According to which, the work of Fed4FIRE+'s Data Protection Officer shall focus on informing, facilitating, coordinating and overseeing the work of testbed-specific Data Protection Officers (to be designated by each testbed owner) which in turn will carry out detailed and context-aware privacy review processes on a yearly basis and ensure the adoption of the aforementioned fundamental principles throughout their respective testbeds.

b) A permanent feedback/review process: which will enable an open discussion on PDP with end-users and shall take place both through surveys and open requests for inputs.

Details for each strategic front will be provided below.

### 4.2.1 Layered PDP strategy

Each testbed in the context of Fed4FIRE+ is managed autonomously by the testbed owner and as such, the platform remains under the control of the latter, for this reason, the appointment of Mandat International as the project's Data Protection Officer (Project DPO) is a necessary but not sufficient condition to have a sound data protection policy and architecture.

Furthermore, it is highly important to remember that testbeds are only provided as a platform for experimenters to perform experiments upon. Neither testbed owners nor testbed DPOs are at any point in the control over the experiments which take place in Fed4FIRE+, their activities are limited to overall control of the testbed and only process a limited range of personal data as necessary to ensure the security and stability of the system, by providing



Co-funded by the Horizon 2020 Framework Programme of the European Union

authentication and identification services to experimenters. In other words, any experimenter that makes use of a Fed4FIRE+ testbed is to be considered a Controller as defined by Article 4 (7) of the GDPR, and as such, they are bound to the obligations set by Article 24 of the GDPR.

Despite not being directed towards the processing of personal data, testbed owners working under Fed4FIRE+ might fall under GDPR Article 4 (8)'s definition of Processors. In this context, testbed owners are not only bound by the obligations of GDPR Articles 25-33, but are also responsible of appointing a testbed-specific Data Protection Officer (Testbed DPO), who will bear the primary responsibility to carry out the activities provided by the applicable data protection law; particularly GDPR Articles 37-39 and the specific primary or secondary normative dispositions of their relevant jurisdiction.

As such, the Testbed DPOs shall:

1) Become a point of contact on Personal Data Protection for each testbed and jointly work with the Project DPO and other testbed DPOs to ensure compliance with the applicable normative framework and the Project's Personal Data Protection Policy, Strategy and Methodology.

2) Inform and advise the experimenters (data controllers) and processor (testbed owner and related team) of their obligations pursuant to the GDPR and to other applicable legal frameworks, particularly as relates to national or sector-specific dispositions which might be relevant to each testbed.

3) Monitor compliance with the GDPR, other applicable legal frameworks and dispositions (whether primary or secondary) and with the policies of the project and testbed in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, experimenters (controllers), and the performance of audits and yearly privacy and security reviews as necessary.

4) To provide advice where requested as regards the data protection impact assessment and monitor its performance in accordance with GDPR Art. 35 (if applicable).

5) To cooperate with the local personal data protection authorities and any other relevant supervisory authority as required.

6) To act as the contact point for the local supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36 of the GDPR, and to consult, where appropriate, with regard to any other matter.

7) To perform all of his/her duties with due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

In order to ensure compliance with the GDPR and relevant national and regional data protection law, the work of these Testbed DPOs shall be coordinated by the Project DPO, who will inform their work, providing any relevant training, information or advice, and jointly working with Testbed DPOs to oversee and facilitate the fulfilment of their obligations whenever possible.

In general terms, the Project DPO's responsibilities will include:



Co-funded by the Horizon 2020 Framework Programme of the European Union

1) Identifying the data sets that are collected by each testbed,

2) Identify the Data Protection Officers that have been appointed by each testbed owner,

3) Request each testbed DPO to perform a privacy and security assessment on a yearly basis (depending on the datasets processed and the individual legal context of each testbed, he might recommend the performance of a full Data Protection Impact Assessment),

4) Organise and coordinate the high-level work or activities to be undertaken among the data controllers (experiment owners), other data subjects, and testbed DPOs involved in the project (particularly as relates to the elements of the permanent feedback/review process),

5) Ensure that clear information is provided on the Project's website regarding the DPOs and the data protection policy of the project.

A graphical illustration of the layered PDP strategy can be found below.

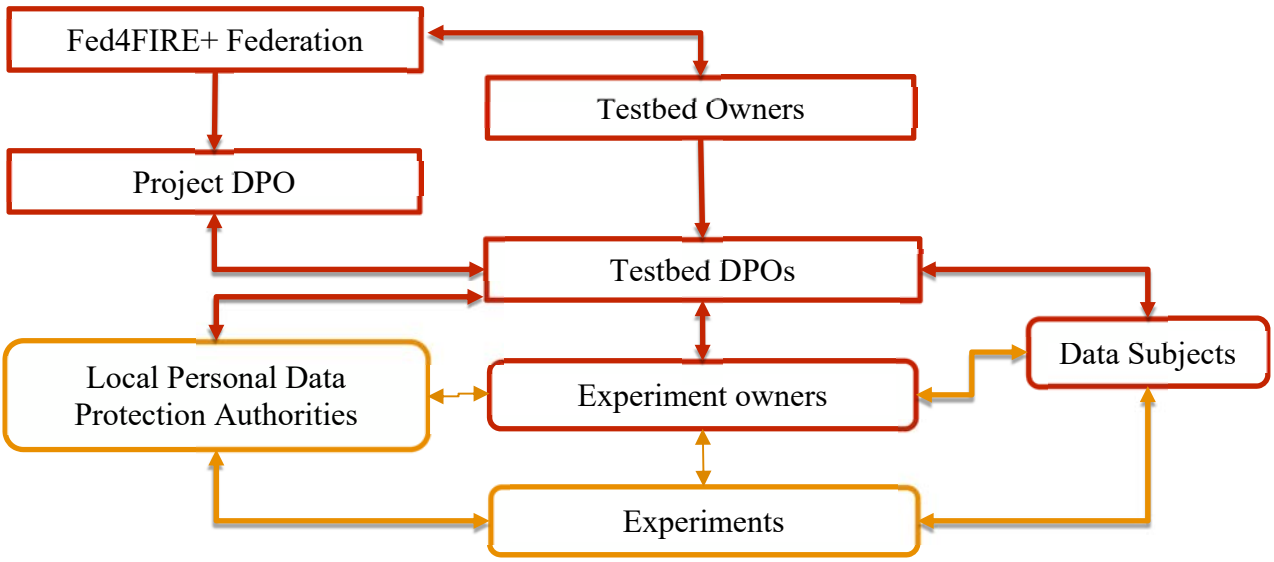


*Figure 2: Graphic illustration of layered Personal Data Protection strategy. In red: Relations directly under the scope of control of the Fed4FIRE+ project; in orange: relations outside the scope of control of the Fed4FIRE+ project.*

### 4.2.2 Permanent feedback/review process

Article 35 (9) of the GDPR recommends controllers to "*seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations*". Considering the visibility and transparency efforts that are not only enshrined in the fundamental principles of the GDPR but also in the Privacy by Design and by Default approach which will be implemented by Fed4FIRE+, the layered PDP strategy will introduce a consequently layered permanent feedback/review process for PDP which will enrich the end-user feedback tasks detailed throughout this Deliverable.

This process shall consist of:



Co-funded by the Horizon 2020 Framework Programme of the European Union

a) **Open communication channels**: generated as a link between experimenters, concerned data subjects and both the project DPO and the testbed DPOs; this mechanism will build upon the basic GDPR requirements for transparency and enable the submission of privacy queries, and other requests for information at any time to the relevant testbed DPO, who might raise the issue to the Project DPO as necessary to provide quick and effective answers or solutions to the privacy and PDP issues raised. In addition to this, consultation mechanisms will be introduced by each testbed owner with regards to every experiment currently running in their platforms.

b) **Consultations** will take two main forms:
   1) Requests for disclosure of PII processing: aimed at ensuring the testbed and the DPO knows whether an experiment involves PII in any way, a request for disclosure of PII processing will be presented to every existing experiment and will be included in the registration form for new experiments.

   2) **Privacy feedback**: which will be circulated among the users of the Fed4FIRE+ systems on a regular manner and will remain available to users to fill on a voluntary basis as part of the user validation activities. Aimed at presenting some basic and open questions to participants regarding their views of the system and the measures that have been implemented to protect their privacy, the forms will also enable the generation of some basic metrics on the transparency efforts introduced while granting the experimenters with the chance to raise questions which will be answered directly by a DPO.

b) **Meetings or workshops with experimenters**: following both the goals of the open communication channels and the results of the information gathered through the consultation mechanisms, both the testbed DPO and the Project DPO will coordinate a series of informative virtual meetings or workshops. Aimed to ensure the clear and transparent dissemination of PDP information among the users of the platform, access to these meetings shall be granted to any interested party, however emphasis will be given to data subjects which consider their data has been processed by the system or their representatives (see GDPR recital 142), and any feedback obtained from them shall be considered when performing the yearly privacy review by both the testbed DPO and the Project DPO.

## 4.3 PERSONAL DATA PROTECTION METHODOLOGY

The PDP methodology consist of:

**1) Open communication channels**

Implementation of open communication channels throughout the platform can take multiple forms. Most commonly, initial contact shall take place through email or by an automated contact form, both of these options shall be made available in the Fed4FIRE+ site and any other public-facing (or available to experimenters) website (as previously mentioned, contact information for both the Project DPO and each testbed DPO shall be published along with the PDP policies of the project in order to comply with the principle of transparency).

Once a request for communication has taken place, the testbed DPO shall take all necessary steps to resolve the question raised, including the coordination of individual or joint calls to address the situation, and the generation of briefings, reports or other relevant documentation as required (while ensuring that such reports do not make vulnerable or affect the PDP rights of any data subject).



Co-funded by the Horizon 2020 Framework Programme of the European Union

### 2) Requests for disclosure of PII processing

The Fed4FIRE+ platform is not aimed to enable the processing of personal data by experimenters, as that could raise the risk of PII breaches and other forms of affectations to the rights of data subjects. In this context, the Terms and Conditions of the platform shall be examined in a joint manner by the Testbed DPOs and the Project DPO to identify a set of changes which clearly defines the scope of PII involved in experiments.

Once this process has concluded and the changes adopted, the platform will only accept those experiments which meet the requirements: the system will ask the experimenter whether or not his experiment involves personally identifiable information, and if given a positive answer, a request for disclosure of the foreseen processing will be presented to the experimenter. In line with this effort, testbeds will contact all current experimenters informing them of the changes in the Terms and Conditions of the platform and requesting them to disclose any processing of PII which could be taking place in their experiments.

Once the disclosure phase has taken place, testbed DPOs will examine the results and, together with the Project DPO will assess whether or not to continue enabling those experiments which involve the processing of PII. This examination shall take particular care to identify and consider any potential risks associated with International Transfers of PII.

### 3) Privacy Feedback

Privacy feedback forms shall be made available for voluntary filling by end-users of the Fed4FIRE+ testbeds, and privacy feedback introduced in the end-user validation tools detailed above through the introduction of open-ended questions aimed to understand the needs and concerns of end-users, as well as to enrich the yearly privacy and security reviews.

Examples of these questions could include:

a) Do you consider you have received sufficient information regarding the way your experiment should address privacy and personal data protection? If no, what information would you like to obtain?

b) Are you aware of any privacy or security risk, vulnerability or concerning element present in the Fed4FIRE+ platform which you would like us to address or to further strengthen?

### 4) Yearly privacy and security review

Ideated as a simplified version of a Data Protection Impact Assessment due to the limited scope of PII processing that has been envisioned to take place in the framework of Fed4FIRE+ (and the additional protection to be implemented through the modification of the platform's Terms and Conditions), this mechanism aims to fulfil a double function:
a) to enable the work of the Program DPO by granting him/her an overview of the technical and organisational measures that have been implemented to safeguard the system's privacy and security,
b) to serve as a baseline document for both the Program DPO and the Testbed DPOs, aimed towards identifying whether individual testbeds (or all of them) should perform a full Data



Co-funded by the Horizon 2020 Framework Programme of the European Union

Protection Impact Assessment in accordance to the requirements specified in Article 35 of the GDPR[5].

Performed on a yearly basis by the Testbed DPOs, the privacy and security review shall be compiled in a written form through the collaboration of all staff members of the testbed and shall take into consideration any feedback received throughout the year by relevant stakeholders. It should build upon previous iterations of the review to identify trends and potential pitfalls for the system, and should also serve to inform the testbed Owner on potential risks and needs of their platforms. The review should be considered as a constantly evolving document, to be updated whenever major changes are introduced to the system, or whenever a vulnerability or data breach has taken place.

Among other, the following questions shall be addressed through the review:

a) What types of personal data are compiled by the platform?

b) What types of personal data are processed by the platform?

c) What types of personal data are published or disseminated by the platform?

d) Which groups of data subjects are concerned when the platform is used?

e) What data flows occur when the product or service is used? (Please provide detailed maps or documentation to reflect the current state of the data flows).

f) What is the area of application of the platform?

g) What is the intended purpose of the platform?

h) Describe the processing operations

i) How is personal data collected by the platform?

j) How is personal data used by the platform?

k) How is personal data retained by the platform?

l) How is personal data deleted by the platform?

m) Does the processing involve marketing? Is there a procedure for individuals to opt-out?

n) How is the accuracy of the personal data ensured by the platform?

o) Will personal data be communicated to other people or stakeholders?

p) How is personal data protected? (Please detail as many technical elements as possible and specify both the technical and organisational protections introduced throughout the life-cycle of the personal data, including the mechanisms to ensure the protection and confidentiality of information at rest and during transmission).

[5] See also CNIL's Manual on how to perform a PIA. Available at https://www.cnil.fr/fr/node/15798



Co-funded by the Horizon 2020 Framework Programme of the European Union

q) Will the project require personal data to be transferred outside of the European Union?

r) How many individuals are affected by the processing?

s) How are individuals informed about the use of their personal data?

t) What reasonable expectations can individuals have with regards to the use of their data by the platform?

u) What assets (hardware, software, networks, people, paper, transmission channels, etc.) which support personal data in the platform?

v) How is informed and unambiguous consent obtained from the data subject?

w) Is the processing of the personal data performed as required for the performance of a contract to which the data subject is a party? Are all types of personal data currently being processed necessary for the performance of contractual obligations?

x) Is the processing necessary and proportionate to the objectives of the platform as declared in the Terms and Conditions?

y) What risks can be associated with the processing of personal data by the platform? How can they be addressed?

z) Is a full Data Protection Impact Assessment necessary?

    a. In particular, does the processing entail two or more of the following:

        i. Evaluation or scoring, including profiling and predicting

        ii. Automated-decision making with legal or similar significant effect

        iii. Systematic monitoring

        iv. Sensitive data

        v. Data processed on a large scale

        vi. Datasets that have been matched or combined

        vii. Data concerning vulnerable data subjects

        viii. Innovative use or applying technological or organisational solutions

        ix. Data transfer across borders outside the European Union

        x. The processing in itself “prevents data subjects from exercising a right or using a service or a contract”

    b. Do any of the exceptions detailed under Article 35 (10) of the GDPR apply?



Co-funded by the Horizon 2020 Framework Programme of the European Union

# 5. COLLABORATION WITH OTHER PROJECTS

Fed4FIRE+ is a 5-year project that will work with other, complementary projects. As a starting point, we have identified three priority projects with which to collaborate:

## 5.1 F-INTEROP

F-Interop is a federation of testbed federations designed to increase online and remote interoperability as well as producing a set of performance test tools that will support emerging technologies. The project promotes the “Testbed as a Service” (TaaS) paradigm as well as standardisation across the industry, which increases efficiency and opportunities in related fields.

The Fed4FIRE+ testbeds will serve as a significant proportion of the testbeds operating under the F-Interop heading. This will increase the service’s reach, improve security for its users, and bring it in line with a common architecture and set of standards.

## 5.2 EXCITING

EXCITING is a collaboration between the EU and China for developing the next wave of mobile technology (5G) and IoT technology. It brings together a series of testbeds across the two regions to help concentrate focus on these technologies and reduce waste of effort among researchers and industry alike.

Fed4FIRE+, as a European testbed project, is in a position to incorporate the testbeds from China under a combination of the Fed4FIRE+ and EXCITING banners. Such collaboration would substantially increase the testing capabilities of Fed4FIRE+ as well as given stronger prominence to the Chinese testbeds in Europe.

## 5.3 IOT LAB

IoT Lab is another federation of testbeds across Europe that specialises in IoT sensor technology and communication between heterogeneous objects and includes tools for crowdsourcing and user surveys.

IoT Lab can work with Fed4FIRE+, ultimately through F-Interop (described above), but also as a means for expanding the capabilities of the TaaS that Fed4FIRE+ represents. It does this by broadening the range of technologies that researchers and other experimenters will have access to through both the IoT Lab and Fed4FIRE+ platforms.



Co-funded by the Horizon 2020
Framework Programme of the European Union

# 6. CONCLUSIONS AND NEXT STEPS

This document presents the Fed4FIRE+ end-user validation roadmap and outlines what data needs to be collected, from whom, in what form, in what manner, how it will be analysed, how recommendations will be made, and how European, national, and regional regulations on privacy and data regulation will be satisfied in the process. It includes a list of tools that will be used for this purpose and sets up contingencies for different eventualities.

Next steps will start with updating the Terms and Conditions of the user agreement to make account of the fact that personal data will be used for validation purposes albeit in a pseudonymised form. These changes will be sent to users to give them an opportunity to decline them. Once that has been done, users will be asked to complete a survey regarding their experiences with the Fed4FIRE+ service. We will collect the responses and simultaneously gather metadata regarding service use.

Once we have these, we will conduct the first round of analysis and recommendations for improvements and general changes to the service.



Co-funded by the Horizon 2020
Framework Programme of the European Union

# REFERENCES


1. EU Network of Independent Experts on Fundamental Rights. (2006, June). Commentary of the Charter of Fundamental Fights of the European Union. European Commission. Retrieved from http://ec.europa.eu/justice/fundamental-rights/files/networkcommentaryfinal_en.pdf
2. European Commission. (2017). The Directive on security of network and information systems (NIS Directive). Retrieved from https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive
3. European Council. Charter of Fundamental Rights of the European Union (2000/C364/01) (2000). Retrieved from http://www.europarl.europa.eu/charter/pdf/text_en.pdf
4. European Parliament, & European Council. Directive 2002/58/EC (as amended by Directive 2009/136/EC) concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (2009).
5. European Parliament, & European Council. Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Retrieved from http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf
6. European Parliament. (2016, July 6). Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union. Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN
7. European Union. (2012, October 26). Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union. Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12012M/TXT&from=en
8. Fed4FIRE+, Description of Action, Part B - Ref. Ares(2016)6428406
9. Federal Assembly of the Swiss Confederation. (1992, June 19). Federal Act on Data Protection (FADP).
10. Swiss Federal Council. (1993, June 14). Ordinance to the Federal Act on Data Protection. Retrieved from https://www.admin.ch/opc/en/classified-compilation/19930159/index.html
11. F-Interop, Annex 1 to the Grant Agreement (Description of the Action) PART B - Ref. Ares(2015)4402355
12. IoT Lab, https://www.iot-lab.info
13. EXCITING, Description of Action, H2020-723227-EXCITING




Co-funded by the Horizon 2020 Framework Programme of the European Union