



Grant Agreement No.: 732638

Call: H2020-ICT-2016-2017

Topic: ICT-13-2016

Type of action: RIA



D2.06 Updated Guidelines on Data Management

Work package	WP 2
Task	T2.7
Due date	30/06/2019
Submission date	31/12/2019
Deliverable lead	Steve Taylor (IT Innovation)
Version	2.0
Authors	Adrian Quesada Rodriguez (Mandat International) & Brecht Vermeulen (IMEC)
Reviewers	Peter van Daele (IMEC) & Lucas Nussbaum (INRIA)

Abstract	This deliverable reports on the data management of Fed4FIRE+ in two significant ways: via Fed4FIRE+'s support for Data Protection in the form of its implementation of GDPR aspects, and Fed4FIRE+'s support for the EC's Open Research Data initiative.
Keywords	Data protection, GDPR, Open Research Data, ORD



DISCLAIMER

The information, documentation and figures available in this deliverable are written by the Federation for FIRE Plus (Fed4FIRE+); project’s consortium under EC grant agreement 732638 and do not necessarily reflect the views of the European Commission.

The European Commission is not liable for any use that may be made of the information contained herein.

COPYRIGHT NOTICE

© 2017-2021 Fed4FIRE+ Consortium

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.



CONTRIBUTORS

Author	Organisation	Section(s)
Steve Taylor	IT Innovation	Sections 1, 3 and 4
Adrian Quesada Rodriguez	Mandat International	Section Error! Reference source not found. , apart from 2.9
Brecht Vermeulen	IMEC	Section 2.9



EXECUTIVE SUMMARY

This deliverable reports on the data management of Fed4FIRE+ in two significant ways: via Fed4FIRE+'s support for Data Protection in the form of its implementation of GDPR aspects, and Fed4FIRE+'s support for the EC's Open Research Data initiative.

A DPO (Data Protection Officer) Network has been established within Fed4FIRE+ consisting of the Project DPO (Mandat International) and individual testbeds' DPOs. The network's purpose is to provide a community and support for the testbed DPOs in dealing with data protection issues.

The primary type of personal information Fed4FIRE+ has to deal with is the registration and login details of experimenters. Fed4FIRE+ operates an identity provider, run by IMEC, which is the controller and collector of this information, and so IMEC's DPO is responsible for this personal information. There is an additional possibility of personal data in Fed4FIRE+, that of personal information included in the data used within an experiment. Support for both types of personal data is discussed.

For Open Research Data, the major conclusion is that the ORD policies and programme integrated with the Open Calls is by and large successful, in that the process is working and opt-in to ORD is strong. At the time of writing, the first results have been prepared and uploaded to the Fed4FIRE+ chosen repository, Zenodo. Future deliverables will provide updated statistics on the continued uptake of ORD in Fed4FIRE+.

Because of the choice of an external ORD storage repository that is well-known, robust and has a long-term chance of survival that is free of charge at the point of use, it has been decided that to conduct risk and cost assessments of long-term data storage is not necessary, and we have proposed an update to the DOA in the July 2019 contract amendment in which this work is removed and replaced by investigations into decision support for GDPR compliance, specifically targeting the multi-stakeholder situations (e.g. an experiment run over multiple testbeds) faced within Fed4FIRE+. This proposed work will not only provide an efficient means to support the testbeds in Fed4FIRE+ but also especially new prospective testbeds wishing to join the federation.

TABLE OF CONTENTS

Disclaimer	2
Copyright notice	2
Acknowledgment	2
Contributors	3
1 INTRODUCTION	9
2 COMPLIANCE WITH PERSONAL DATA PROTECTION	10
2.1 Personal Data Protection (PDP) Strategy for Fed4Fire+	10
2.1.1 Layered Personal Data Processing (PDP) Strategy	10
2.1.2 Permanent feedback/review process	13
2.2 Implementation Report	14
2.2.1 PDP Strategy	14
2.3 Relevant Data Protection Regulations for FED4FIRE+	18
2.4 Key GDPR Principles	18
2.5 Key E-Privacy Directive Principles.	22
2.6 General Privacy Requirements and Summary of Initial Implementation in FED4FIRE+	23
2.7 Specific Data Protection Requirements and Summary of Initial Implementation in FED4FIRE+	24
2.8 Relevant Privacy Risks, Recommended Risk Mitigation Measures and Initial Implementation Report	27
2.9 Fed4FIRE Experimenters and Privacy Statements	28
2.9.1 Fed4FIRE account	28
2.9.2 Fed4FIRE experiments on testbeds	30
2.9.3 Examples of experiments with personal data	32
2.10 Conclusion	32
3 OPEN RESEARCH DATA	33
3.1 Integration of Open Research Data into Open Calls	33
3.2 ORD Take-Up in Open Calls	34
3.2.1 Open Call 3	34
3.2.2 Open Call 4	36
3.2.3 Open Call 5	37
3.2.4 Open Call 6	38
3.2.5 Continuous SME Call	39
3.3 Risk Analysis of Long-Term Storage of Open Research Data	39
3.4 Proposal for Contract Amendment – GDPR Decision Support for Experimentation Platforms	41



4	CONCLUSIONS & NEXT STEPS	43
5	APPENDICES	44
5.1	Open Call Information	44
5.2	Experiment Proposal Template	45
5.3	Experiment Report Template	46



LIST OF FIGURES

Figure 1 : 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 13

Figure 2: Screenshot Fed4FIRE+ portal – Indication link to privacy statement 28

Figure 3: Screenshot Fed4FIRE+ portal – Requirement for approval of terms and conditions and privacy statement 29

Figure 4: Warning by jFed if user has not agreed with terms and conditions and privacy terms of the testbeds he/she wants to use..... 30

Figure 5: Testbed specific terms and conditions and privacy statements are maintained and hosted by the specific testbeds (example of the IRIS testbed policy)..... 31

Figure 6: OC3 Open Research Data Take-Up 34

Figure 7: OC4 ORD Statistics 36

Figure 8: OC5 ORD Statistics 37

Figure 9: OC6 ORD Statistics 38



LIST OF TABLES

Table 1: Fed4FIRE Testbed Data Protection Officers (DPOs)	15
Table 2: Privacy Risks and Mitigation Measures	27



1 INTRODUCTION

This is the second in a series of deliverables concerning data management in Fed4FIRE+. It follows from D2.1, authored mid-2017, which contained two major sections: guidance for GDPR compliance in Fed4FIRE+ experiments, and support for Open Research Data in Fed4FIRE+ experiments. This deliverable follows a similar structure.

The deliverable begins by providing an updated view on the personal data protection requirements stated in D2.1 and the personal data protection strategy found in the deliverable on end-user validation. To this end, it restates the requirements, updates them whenever necessary, and details the actions and controls undertaken by all members of the Data Protection Officer network (DPO Network) of Fed4Fire+ to ensure compliance with the GDPR.

The Open Research Data (ORD) section describes how the policies, processes and templates for ORD support within Fed4FIRE+ that were proposed in D2.1 have been implemented and incorporated in Fed4FIRE+'s processes and practices for experiments. There has been no need to modify the policies or processes recommended in D2.1, and therefore this section describes the implementation, as well as the uptake by experimenters when they were given the option to make their experiment data open

This deliverable was originally authored in June 2019, but its submission has been delayed for a number of reasons:

- Firstly, so as to provide the latest statistics regarding uptake of the Open Research Data policies and processes instigated in the project. To keep to the initial submission date of the deliverable would have meant that few experiments featuring ORD support would have been completed so the success of the ORD support would not have been known at this time.
- Secondly, to provide details and justification on the contract amendment proposed over summer 2019 that has direct relevance to the T2.7 Data Management task.
- Finally, to report on the new Fed4FIRE+ portal, which was developed at IMEC over summer 2019. This is a single-sign-on portal where registration information is collected and is therefore main point of contact for the collection of personal information for Fed4FIRE+.

As a result of the desire to report on these activities, this deliverable has been updated over the summer of 2019 and its submission delayed so that this information may be provided. There is no work that depends on this deliverable that needed to happen in the delay period, so the project's progress has not been compromised.

2 COMPLIANCE WITH PERSONAL DATA PROTECTION

2.1 PERSONAL DATA PROTECTION (PDP) STRATEGY FOR FED4FIRE+

As reported in D2.10, the Fed4Fire+ deliverable on end-user validation, in the context of the efforts towards ensuring Fed4FIRE+ fully complies with the relevant data protection regulations described below, the following general strategy will be pursued through its upcoming phases. Firstly, Mandat International (MI) will adopt a vigilant role throughout the initial phases to ensure that personal data collection is performed in accordance with the GDPR and respecting the rights of the data subjects. Once the architecture is stabilized, a Privacy Impact Assessment will be performed, and once completed, each identified risk will be addressed with adequate mitigation measures; this approach will be further complemented with the regular monitoring of the infrastructure by the partners and Data Protection Officer (DPO) of each testbed. Finally, third party end-users of the platform will be invited to assess the personal data protection and the platform services through the diverse stages of the process.

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

- ➔ A layered strategic approach to Personal Data Protection (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.
- ➔ 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.

To assist in achieving these aims, a "DPO Network" has been established within Fed4FIRE+ consisting of the Project DPO (Mandat International) and individual testbeds' DPOs. The network's purpose is to provide a community and support for the testbed DPOs in dealing with data protection issues.

Details for each strategic front will be provided below.

2.1.1 Layered Personal Data Processing (PDP) Strategy

Each testbed in the context of Fed4FIRE+ is managed autonomously by the testbed owner and as such, the platform remains under their control. 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 authentication and identification services to experimenters.

As a result of this discussion, we have determined the two key scenarios where personal data is relevant in Fed4FIRE+.



1. Personal data is used for registration of Fed4FIRE+ experimenters by the Federator. The personal data is used for the purposes of creation of access tokens (e.g. SSH) keys, which may be used to access the testbeds in the federation. Testbeds may additionally register users themselves and while this is strictly beyond the scope of Fed4FIRE+, similar responsibilities regarding data protection need to be observed by the testbeds.
2. Any personal data within an experiment. This case is strictly the responsibility of the experimenter. In other words, any experimenter whose experiment uses personal data 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. Although the experimenter must bear the responsibility for the data protection aspects of their experiment, Fed4FIRE+ acknowledges that experimenters are not necessarily experts in data protection and can provide guidance and training for experimenters who wish to use personal data within their experiments.

In this context, two levels of information and interactions with experimenters can be expected:

- ➔ Information and awareness activities handled in the context of Fed4Fire+ (in which Fed4Fire+ experimenters will be provided a general training about the GDPR requirements and informed of the data processing requirements defined by the testbeds, to be carried out by the Project DPO in agreement with the Federation board); and
- ➔ information, awareness and contractual interactions carried out by testbeds outside of the context of Fed4Fire+ (which are not controlled by the Project DPO or the DPO network).

Given the experiments run on Fed4FIRE+ testbeds and that any experimenter whose experiment involves personal data is deemed a Data Controller for their experiment, 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. Testbeds also register users, whose personal data needs to be protected and managed. These reasons oblige testbeds to appoint a Data Protection Officer for their testbed (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 the experimenters (data controllers) and processor (testbed owner and related team) of the testbed's position regarding processing of personal data in their infrastructure, introducing individual policies or data processing agreements as necessary (both through the testbed's website and through the dedicated jFed privacy policy extension); and comply with 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 reports 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.

As part of these activities, the jFed GUI has been extended to be able to display the individual privacy and data processing policies of each testbed, which will be noted by the DPO network. Furthermore, the experiment proposal template will be updated to require experimenters to state whether their experiment contains any personal data.

➔ If the answer is YES

- Any testbed that has stated that they are unwilling to process personal data will be ruled out of participating in that experiment.
- The experimenter will be required to confirm that they will be a Data Controller for all data processed within their experiment, and that they understand, and will comply with, all the relevant requirements of the GDPR.
- The experimenter will be required to interact with the testbeds of their experiment, as the testbeds are acting as Data Processors under the instruction of the experimenter as data controller for their experiment.

➔ If the answer is NO

- The experimenter will be required to guarantee that no personal data is included within the experiment's data, either provided initially or generated throughout the course of the experiment.
- All testbeds are eligible to participate within this experiment.

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:

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 1).

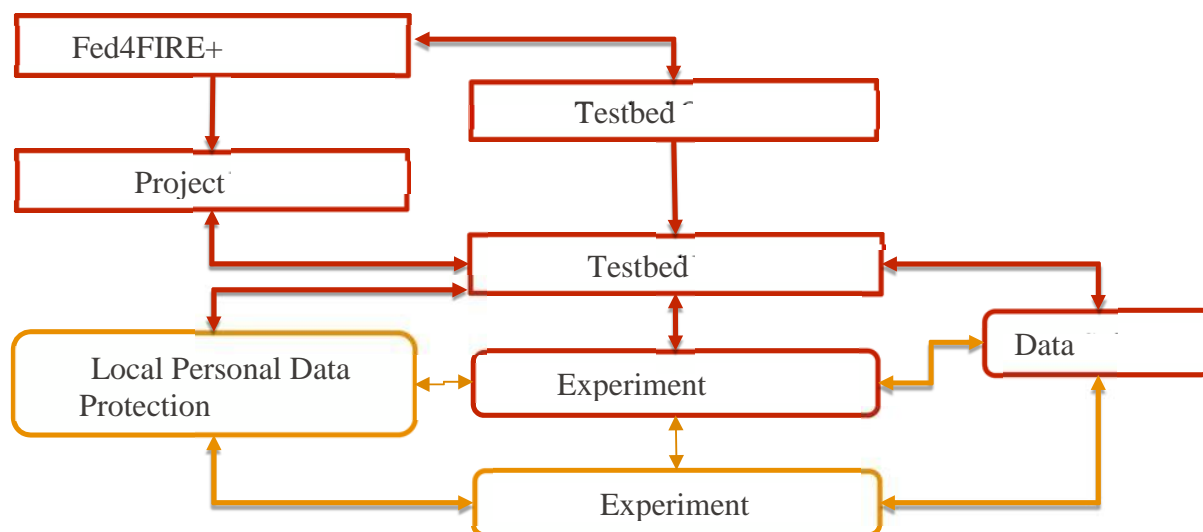


Figure 1 : Graphic illustration of layered Personal Data Protection strategy. In red: Relations directly under the scope of control of the Fed4FIRE+ project; in orange: relations outside the scope of control of the Fed4FIRE+ project

2.1.2 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 is carried out in the framework of the end-user validation activities in Fed4Fire+ and is envisioned to consist generally of:

- ➔ 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.
- ➔ Consultations which will take two main forms:
 1. Requests for disclosure of Personal Data processing: aimed at ensuring the testbed and the DPO knows whether an experiment involves Personal Data in any way, a request for disclosure of Personal Data processing will be presented to every existing experiment and will be included in the experiment proposal template for new experiments.
 2. Privacy feedback: questionnaires 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 questionnaires 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.

- ⇒ 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.

2.2 IMPLEMENTATION REPORT

2.2.1 PDP Strategy

The PDP strategy detailed above has been followed through by all Fed4Fire+ partners. After an initial call for the designation of Testbed DPOs in early 2018. Bi-monthly DPO network calls have been carried out by the network.

The current list of testbed DPOs is given in Table 1, below:



Table 1: Fed4FIRE Testbed Data Protection Officers (DPOs)

Testbed	Location	Owner	Type	DPO	Email
NITOS	Greece	CERTH	Wireless / 5G / IoT	Stavroula Maglavera	stavmag@the.forthnet.gr
FuSeCo	Germany	FOKUS	Wireless / 5G / IoT	Alexander Willner	alexander.willner@fokus.fraunhofer.de
OFELIA island	Spain	i2CAT	OpenFlow	Sonia Beltrán Cesario	sonia.beltran@i2cat.net
Virtual Wall	Belgium	IMEC	Wired networking	Brecht Vermeulen	Brecht.Vermeulen@ugent.be
w-iLab.t	Belgium	IMEC	Wireless / 5G / IoT	Brecht Vermeulen	Brecht.Vermeulen@ugent.be
Portable wireless testbed	Belgium	IMEC	Wireless / 5G / IoT	Brecht Vermeulen	Brecht.Vermeulen@ugent.be
City of Things Antwerp testbed	Belgium	IMEC	Wireless / 5G / IoT	Brecht Vermeulen	Brecht.Vermeulen@ugent.be
Virtual Wall	Belgium	IMEC	OpenFlow	Brecht Vermeulen	Brecht.Vermeulen@ugent.be
Virtual Wall (including GPUlab)	Belgium	IMEC	Cloud computing	Brecht Vermeulen	Brecht.Vermeulen@ugent.be
Tengu	Belgium	IMEC	Big Data	Brecht Vermeulen	Brecht.Vermeulen@ugent.be
Grid5000	France	Inria	Cloud computing	Lucas Nussbaum	lucas.nussbaum@loria.fr
LOG-a-TEC	Slovenia	JSI	Wireless / 5G / IoT	Igor Ozimek	

D2.06 Updated Guidelines on Data Management



Netmode	Greece	NTUA	Wireless / 5G / IoT	Dimitris Dechouniotis	ddechou@netmode.ntua.gr
PL-LAB	Poland	PSNC	Wired networking	Tomasz Nowocień	nowocien@man.poznan.pl
IRIS	Ireland	TCD	Wireless / 5G / IoT	Diarmuid Collins	collindi@tcd.ie
SmartSantander	Spain	UC	Wireless / 5G / IoT	Luis Muñoz	luis@tmat.unican.es
PerformLTE	Spain	UMA	Wireless / 5G / IoT	Alvaro Rios	alvarorios@lcc.uma.es
PlanetLab Europe	France	UPMC	Wired networking	Agnieszka Wrzesień-Gandolfo	agnieszka.gandolfo@lip6.fr
Exogeni	Netherlands	UvA	Cloud computing	Kees Koppenol	C.L.Koppenol@uva.nl



The first action point of the network was focused on information and coordination activities: Testbed DPOs were invited to discuss their roles, and to assess the testbed's position regarding processing of personal data in their infrastructure. To compliment this, testbed owners who had not yet appointed a DPO were presented with the general outline of the GDPR and the obligations it would introduce to their system. This was followed by an analysis of the most viable risk mitigation strategy to be pursued by Fed4Fire+ to avoid GDPR violations when an experimenter carries out personal data processing in a testbed. Several options were examined, and a draft contract was discussed as a possible option. Finally, a more practical approach was pursued by all testbeds, as they are individually tied to the GDPR obligations and to specific national laws and regulations. The approach chosen involved IMEC introducing an extension to the jFed tool which enables the testbeds to require experimenters to agree to their individual privacy and data processing policies. Finally, internal compliance controls have been put in place to minimize the potential impact of any non-compliance in a testbed towards the Fed4Fire+ project. All testbeds have been required to provide a signed declaration of their actions towards compliance and the rationale that supports such actions.

The DPO network is currently maintaining high levels of activity. The most recent action undertaken included requesting contractually binding disclosure from testbed owners of the measures undertaken thus far to implement the GDPR requirements. Future work includes a cross-examination of security mechanisms and the development of best practices to be introduced, alongside with an updated examination of the measures introduced by testbeds, which have been already analysed as part of the feedback and review process detailed below. Additionally, the Federation board will be invited to support training for current and future experimenters on the GDPR and their eventual role as data controllers.

Permanent feedback/review process:

- ➔ Open communication channels: Experimenters are encouraged to contact the Fed4Fire+ DPO, the DPO network and the testbed DPOs if any questions arise on the processing of their personal data, this is particularly true during FEC meetings, when the project DPO is able to respond to the questions directly. Additionally, testbeds have introduced their own communication channels to their respective DPOs and, in case the questions receive relate to the Fed4Fire+ project, they will share this information with the DPO network to answer the issues.
- ➔ Consultations: The jFed tool has been modified to introduce a tool to enable testbed owners to introduce disclosure policies in their privacy and data processing agreements, which will be shown to experimenters before they can begin to utilize the testbed infrastructure. With regards to the feedback mechanisms, they have been carried out as part of the end-user validation activities of Fed4Fire+ and their results will be reported on a separate deliverable, however no major issue has been detected thus far.
- ➔ Meetings or workshops with experimenters: This option is offered to experimenters and if needed will be carried out in future FECs if considered relevant by the consortium and the DPO network. The option to carry out this activity will be discussed by the DPO network, particularly in order to carry out the yearly privacy reviews.



2.3 RELEVANT DATA PROTECTION REGULATIONS FOR FED4FIRE+

Following Article 16 of the Treaty on the Functioning of the European Union, which is the legal basis for the adoption of data protection rules in the EU, the European Union legislator adopted the Regulation 679/2016 (hereinafter “GDPR”) to protect the fundamental right to data protection and to guarantee the free flow of personal data between Member States. The logic of the adoption of a GDPR was to prevent disparities between Member States in terms of procedures and sanctions, harmonizing the data protection in the EU.

This Regulation is complemented by Directive 2002/58/EC on privacy and electronic communications (ePrivacy Directive), which concerns the processing of personal data and the protection of privacy in the electronic communications sector and states specific requirements concerning the protection of personal data and privacy of the users of electronic communication services. In the context of Fed4FIRE+, the following principles are of relevance:

2.4 KEY GDPR PRINCIPLES

This section describes key GDPR principles together with a description of how Fed4FIRE+ addresses them. In this and the following sections, Fed4FIRE+ measures to address GDPR principles and requirements are highlighted in **blue text**.

1. The GDPR applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.
 - In the context of Fed4Fire+, this principle applies in two cases, namely:
 - Fed4Fire+ end-user (experimenter) personal data: personal details about the experimenters, used is used by Fed4FIRE+ (and IMEC in particular) to allow them to run experiments (authentication/authorization for the jFed tool)
 - Third-party personal data: Data about third-party data subjects which could be processed in any of the testbeds as part of experiments. This personal data is not under the control of Fed4Fire+ or the testbed owners, as the controller would be the experimenter. Processing of this personal data within a testbed requires that testbed to act as a Data Processor, under the instruction of the experimenter in their role as a Data Controller. As described below, several actions are underway to enable the GDPR-compliant processing of personal data in a Fed4Fire+ experiment, both on a project-level and on a testbed-level.
2. The GDPR has an extra-territorial reach, meaning that its rules apply not only to controllers or processors established in the European Union, but also to entities having their establishment in a third country, if they:
 - a. Offer goods or services, irrespective of whether a payment of the data subject is required, to data subjects in the Union (e.g. a US-based social network); or
 - b. Monitor the data subjects’ behaviour, as far as their behaviour takes place within the Union (e.g. email tracking service providers)
 - In the context of the project, these requirements pertain to the personal data of jFed users which is used to access a testbed not located in Europe, which would still be protected under the scope of the GDPR. It is important to acknowledge that under some circumstances, SSH keys could be considered to be personal data.

3. Personal data cannot be processed without a legal ground. This usually entails that the data subject has to give his/her consent to the processing of his or her personal data for one or more specific purposes; however, different legal grounds may apply, in different instances, which could exempt controllers or processors from collecting the data subject's consent. This holds true when personal data processing:
 - a. is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract (e.g. when transferring connected cars' data to an external provider of maintenance services, as agreed with the car's owner through a contract);
 - b. is necessary for compliance with a legal obligation to which the controller is subject (e.g. a Union, national or regional law setting out rules and obligations for cities within smart cities' programs);
 - c. is necessary in order to protect the vital interests of the data subject or of another natural person (e.g. when deploying IoT devices for emergency health care purposes);
 - d. processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (e.g. when personal data processing is necessary to manage a tax system);
 - e. processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child (the discipline of the legitimate interest still vary across EU Member States and needs a case by case assessment).
- In the context of Fed4Fire+, processing of the experimenters' personal data is carried out for authentication/authorization purposes towards the performance of a contract between IMEC and the experimenters or towards complying with the obligation of securing the systems from threats. Specific privacy policies and other relevant information on the legal basis for the processing activities can be identified in the privacy statement of both IMEC and Fed4Fire+. For the case where personal data is embedded in an experiment, the experimenter in their role as Data Controller is responsible for determining the lawful basis, which will be specific to the purposes of the experiment. Often the lawful basis will be consent, but Fed4FIRE+ can provide guidance to experimenters as to which lawful basis is most appropriate given the circumstances of the experiment in question.
4. Consent should be free, unambiguous, informed, prior and demonstrable by the data controller, meaning that it must be documented somehow (also electronically, e.g. by means of a log).
 - In the context of Fed4Fire+, consent is required from experimenters at the moment of registration (described in detail in Section 2.9). Information is presented at several stages of this process.
5. In any event, data subjects must be informed about the processing undergone by their personal data before the processing starts or, when data are not collected from the data subjects themselves, within a reasonable period, in any event no later than the first communication or the first disclosure to the public, when such activities are foreseen (e.g. in a smart city context, by complete information notices published on the cities' websites, by icons displayed on the users' devices, by signs on the street in correspondence of IoT sensors or cameras).



- For experimenters, personal data processing is carried out in Fed4Fire+ to carry out the authentication and authorization activities, and the experimenters are informed about what processing will take place at the point of registration. If any new data processing is envisioned in the framework of the project, this will not take place without the end-user consent and information. For the case where personal data is embedded in experiment, the experimenter (as Data Controller) needs to ensure that the data subjects are adequately informed and Fed4FIRE+ can provide support to experimenters to ensure that the correct measures are in place.
- 6. Data protection principles (i.e. data minimization, purpose limitation, data accuracy, storage limitation etc.) must always be respected; a data controller may have a legal ground to process personal data (e.g. the data subject's consent), yet it may still run the processing in breach of one of the key data protection principles, which would make the personal data processing unlawful and, potentially, trigger a sanction by competent authorities. This is the essence of the principle of accountability.
- Data protection principles are respected by all Fed4Fire+ testbeds as they are all legally bound by the GDPR. The DPO network seeks to ensure accountability: Fed4Fire+ testbeds have been required to provide a signed declaration acknowledging the information received regarding Personal Data Protection and GDPR compliance requirements; as part of these declarations they have disclosed the actions undertaken to comply with the requirements as well as any circumstances that prevent them from doing so. The declarations are not disclosed as part of this deliverable given the sensitive nature of the information contained therein.
- 7. The principle of data protection-by-design is now set in law. It requires the controller to implement “technical and organizational measures appropriate to the processing activity being carried out and its objectives, such as data minimization and pseudonymisation, in such a way that the processing will meet the requirements of [the] Regulation and protect the rights of (...) data subjects”;
- The design of Fed4Fire+ facilitates the implementation of privacy by design and by default, as, in principle no personal data of experimenters is shared between the testbeds (the jFed tool utilizes only SSH keys for authentication and authorization purposes, which are provided by IMEC, who serves as sole data controller over end-user personal data). The DPO network seeks to ensure privacy is considered in the development of any new applications or functionalities to be introduced to Fed4Fire+.
- 8. The same goes for the principle of data protection-by-default, that refers to the amount of data collected, retention period, extent of the processing, data accessibility etc. Essentially, “the controller shall implement appropriate measures for ensuring that, by default, only (...) personal data (...) which are necessary for each specific purpose of the processing are processed”.
- The Fed4FIRE+ federator collects personal data for registration and authentication of user identity purposes, and the data collected is limited to that needed for this purpose. Testbeds also register users outside of Fed4FIRE+ and, although this purpose is outside the scope of Fed4FIRE+, the testbeds have committed to protecting the privacy of their users, so are expected to collect minimised data as well. For the case where personal data is embedded in an experiment, the purpose for which it is collected and processed cannot be known a priori and is in any case the responsibility of the experimenter in their role as Data Controller. Fed4FIRE+ will work with experimenters to provide support for determining the appropriate types and amount of personal data given the purposes of an experiment.

9. Clear procedures must be in place to ensure data subjects' rights, namely:
 - a. Right of access;
 - b. Right to rectification;
 - c. Right to erasure;
 - d. Right to restriction;
 - e. Right to data portability
 - f. Right to object
- IMEC has a standard policy for the protection of its users' rights, given in its standard privacy statement ¹, which is presented to users at the point of registration.
10. Procedures to handle and notify Data Breaches to Data Protection Authorities and Data Subjects concerned must be in place.
 - All testbeds are aware of the requirement to notify data breaches they might suffer, both to the DPO network and the relevant Data Protection Authorities, along with the Data Subjects in accordance to the GDPR.
11. Stakeholders must delete raw personal data as soon as they have extracted the data required for their data processing.
 - Data deletion and minimization are integrated in the Fed4Fire+ models, particularly by IMEC as data controller of the personal data used for authentication and authorization.

As detailed further below, these principles have all been integrated in the Fed4Fire+ processes and are required both from testbed owners and experimenters.

¹ <https://www.imec-int.com/en/privacy-statement>

2.5 KEY E-PRIVACY DIRECTIVE PRINCIPLES.

1. Where the ePrivacy Directive ² provides for a specific rule applicable to natural and legal persons in relation to processing in connection with the provision of publicly available electronic communications services in public communication networks, it prevails over the general rule set out by the GDPR (“Lex Specialis derogat generali” - Principle of Specialty);
2. Electronic Communication Services and Networks must be secured through appropriate technical and organizational measures (Security);
- None of the testbeds currently under Fed4Fire+ provide services which might fall under the definition of an electronic communication service and network as described in Art. 3 of the ePrivacy Directive: “This Directive shall apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community”.
3. The confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, must be ensured (Confidentiality);
- This principle is respected by all Fed4Fire+ partners, as it is an extension of the GDPR requirements.
4. Access to, or storage of, information into the users’ devices must be authorized by the users with a specific consent, unless it is “strictly necessary in order to provide a service explicitly requested by the subscriber or user” (also known as “cookie law”, Prior Consent);
- Installation of the jFed tool can only be carried out under the specific consent of the end-user and in the context of the services that have been requested by the experimenters.

Based on these principles, the testbeds under Fed4fire+ have, whenever applicable, introduced the necessary actions to prevent eventual breaches. Furthermore, an examination of the latest draft of the ePrivacy Regulation is currently underway and will be reflected in the work of the DPO network in case it introduces any relevant requirements

² See <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058>



2.6 GENERAL PRIVACY REQUIREMENTS AND SUMMARY OF INITIAL IMPLEMENTATION IN FED4FIRE+

The design of the system architecture is a crucial phase to ensure the security and privacy of the information processed therein. In fact, according to the GDPR, *“the controller should adopt **internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default**. Such measures could consist, inter alia, of **minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features**. When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations”*.

Moreover, the system must be embedded with **appropriate technical and organizational measures to ensure a level of security appropriate to the risk**, including inter alia as appropriate:

- **the pseudonymisation and encryption of personal data:** which is obtained in Fed4Fire+ at different levels, including the pseudonymization and encryption of user accounts, the activities of the experimenters and when reporting results of the project.
- **the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services:** confidentiality and integrity are supported by security mechanisms introduced by the diverse testbeds (and examined both by the DPO network and by the external validation and audit process carried out by IMEC); availability is guaranteed by the distributed nature of the federation, the different security mechanisms utilized by all the testbed owners and the resilience reports generated by the jFed tool (where end-users can see the overall health status of each testbed).
- **the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident:** Fed4Fire follows a data minimization approach, under which no unnecessary personal data is handled or managed by the testbeds. The jFed tool processes personal data in order to generate a user account and create an SSH key for authentication and authorization purposes. In this context, the availability and access work is greatly simplified, as the data subject does not see an impairment of their access to the work done on the platform in case an availability breach takes place.
- **a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing:** Each Fed4Fire+ testbed has processes in place to test, assess and evaluate their own technical and organizational security measures, and these processes are coordinated through the work of the DPO network. This information is not made publicly available in this deliverable due to security but can be made available under restriction upon request.
- **policies and procedures to periodically test the security resilience of a system** (e.g., penetration tests, vulnerability assessments, etc.) and carry out the relevant remediation activities: As detailed before, these actions take place at the discretion of each testbed owner and should be reported back to the DPO network in case any major issue is found.
- **a well-defined internal procedure to alert the system administrators when any data breaches take place:** The DPO network has an alert system in place for communicating issues to the Project DPO and to IMEC as organization in charge of the jFed tool (which is the only element that handles personal data of the experimenters).



Fed4FIRE+ aims to ensure the systematic adaptation and improvement of its experimentation framework to fully comply with the personal data protection principles. Following an examination of these principles, the following Privacy Requirements (“PR”) are drawn from the GDPR amongst those relevant for Fed4FIRE+. These requirements are adapted to the foreseen architecture, based on the two use cases of personal data usage (registration of users and experiment-specific personal data). Even though experiment-specific personal data is the responsibility of the experimenter, the Fed4Fire+ DPO network will continue to analyse how to address the risks and opportunities raised by experimenter-led processing of personal data and will jointly support activities which enable experimenters to confidently manage the requirements of the GDPR in their experiments.

2.7 SPECIFIC DATA PROTECTION REQUIREMENTS AND SUMMARY OF INITIAL IMPLEMENTATION IN FED4FIRE+

- ➔ **Project data management:** The system must automatically record all internally generated data, storing these data into the Fed4FIRE+ platform, while minimizing the collection of personal data.
- **Implementation:** data minimization has been implemented as a high-priority requirement by all testbed owners as part of their individual GDPR compliance activities. The testbeds’ main purpose of processing personal data is for registration of users and the data they collect is limited to that needed for this purpose. Personal data management is carried out by IMEC under their own internal policies subject to the GDPR and direct communication with the project DPO is in place in case any issue arises.
- ➔ **Data back-ups:** Back-up operations will be carried out periodically, so as to ensure the continuity of the system and prevent the loss of data.
- **Implementation:** The Fed4Fire+ federation is distributed by design and no personal data of experimenters are transferred within the federation partners which might require backup. IMEC, as controller of the personal data of jFed users has introduced sufficient security mechanisms and organizational processes as part of their compliance activities with the GDPR to comply with this requirement.
- ➔ **Authentication of identities:** The whole system will collect different types of data and it will be designed to ensure the privacy and trust of the users. In order to do this, each identity accessing the system will be authenticated and appropriately authorised to be able to use it. Where necessary (e.g. when the system is used to process health data), strong authentication (e.g. two-factor authentication, double opt-in, biometric recognition, etc.) methods must be supported.
- **Implementation:** the jFed tool run by IMEC introduces this functionality, by generating the SSH key of the experimenter it enables proper authentication functionalities across the federation.
- ➔ **De-activation of authentication credentials:** Personal authentication credentials shall be de-activated if they have not been used for at least six months (except in case of technical authorization).
- **Implementation:** This requirement has been transmitted to IMEC, implementation of credential deactivation has been introduced, however account deletion requires end-user feedback as some experiments might require the account to continue existing over time.

- ➔ **Purpose limitation:** As set out by article 5 of the GDPR, Fed4FIRE+ will process personal data only for security purposes, unless the data controller configures the system to pursue other legitimate, specific and explicit purposes, determined at the time of collection of the data.
- **Implementation:** at a project level, the principle of data minimization is followed. IMEC is the controller of personal data for Fed4FIRE+ experimenter registration and has a sufficiently strong privacy policy³ to convey the purposes and exact limits of the processing they will carry out. This personal data is only used for authentication and authorization processes and is not disclosed to any party whatsoever.
- ➔ **Data accuracy and updating:** Personal data which are inaccurate or incomplete, having regard to the purposes for which they were collected or processed, will be erased or rectified as set out by article 5 of the GDPR.
- **Implementation:** IMEC provides mechanisms for users to correct their personal data and additionally has manual check-up processes carried out after signup, and extra information might be asked if the new user is not known by an out of band mechanism.
- ➔ **Security of processing:** Fed4FIRE+ will protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access through the implementation of technical and organisational measures as required by article 32 of the GDPR.
- **Implementation:** IMEC, as data controller of the experimenter registration data processed by the jFed tool, has introduced dedicated data security mechanisms and organizational compliance activities, which have been clearly specified in the organizational policies of Ghent University. Security audits are carried out as necessary to ensure compliance with all relevant requirements. So far no security breaches have taken place.
- ➔ **Data breach information:** The Fed4FIRE+ system must immediately inform its users of any breach to personal data leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed as required by articles 33 and 34 of the GDPR.
- **Implementation:** IMEC has data breach policies currently in place. These are not disclosed in this deliverable for security reasons. So far, no data breaches have taken place in Fed4FIRE+.
- ➔ **Encryption by default:** As provided by Article 32 of the GDPR, encryption will be applied to all stages of handling data, including in communication, storage of data at rest, storage of keys, identification, access, as well as for secure boot process.
- **Implementation:** Security is taken extremely seriously by Fed4FIRE+. All communication and APIs are carried out over SSL. The servers containing the databases holding personal information are behind a firewall, and get frequent updates. The sysadmin team having access to the servers is limited to the minimum.
- ➔ **Right of access:** The Fed4FIRE+ system shall support the data controllers in providing to every data subject, without excessive delay or expense, confirmation as to whether or not data relating to him/her are being processed and information as to: the purposes of the processing; the categories of data concerned; the recipients to whom the data are disclosed; the envisaged period of storage for the data; and the existence of automated decision-making processes within the system. The legal source of this requirement is article 15 of the GDPR.

³ <https://www.imec-int.com/en/privacy-statement>

- Implementation: Data access rights have been detailed in the Fed4Fire+ project and have been introduced by IMEC as part of their organizational policies. IMEC has a standardised mechanism for users to request the personal data held on them. Testbeds are able to introduce addendums or specific personal data protection policies to the jFed tool in order to detail how to deal with SSH key processing or specific requirements for processing personal data as part of experiments (and disclaimers preventing experimenters from carrying out such processing).
- ➔ **Right of erasure:** The Fed4FIRE+ platform must ensure that the right of erasure exercised by data subjects towards the data controller is enforced, when the conditions set out by article 17 of the GDPR are met.
- Implementation: Testbed owners have introduced specific dispositions to comply with this requirement at an internal level. IMEC, as lead of the jFed tool, has introduced this right in their organizational policies.
- ➔ **Data portability:** As detailed by article 20 of the GDPR, the Fed4FIRE+ platform must be able to support the data controller in responding to requests for data portability lodged by the data subjects. This entails that the data subject shall receive the data in a structured, commonly used and machine-readable format.
- Implementation: data portability has, so far, not been a key issue for the Fed4FIRE+ project. Considering the nature of the authentication mechanism, which is currently handled by IMEC, users are able to utilize multiple testbeds using a single SSH key. Despite this situation, both personal and non-personal data portability is a topic that will be considered in accordance with the Fed4Fire+ DOA.
- ➔ **Regular monitoring of security:** The Fed4FIRE+ platform will regularly monitor the system's status in terms of security for personal data as required by article 32 of the GDPR.
- Implementation: regular security monitoring is carried out by all testbeds as part of their individual compliance activities. In the specific case of IMEC, as data controller, they have introduced monitoring and audit processes which regularly review the security of their systems.

2.8 RELEVANT PRIVACY RISKS, RECOMMENDED RISK MITIGATION MEASURES AND INITIAL IMPLEMENTATION REPORT

A number of privacy risks can be identified and mitigation measures must be implemented to tackle each risk. These are shown below in Table 2

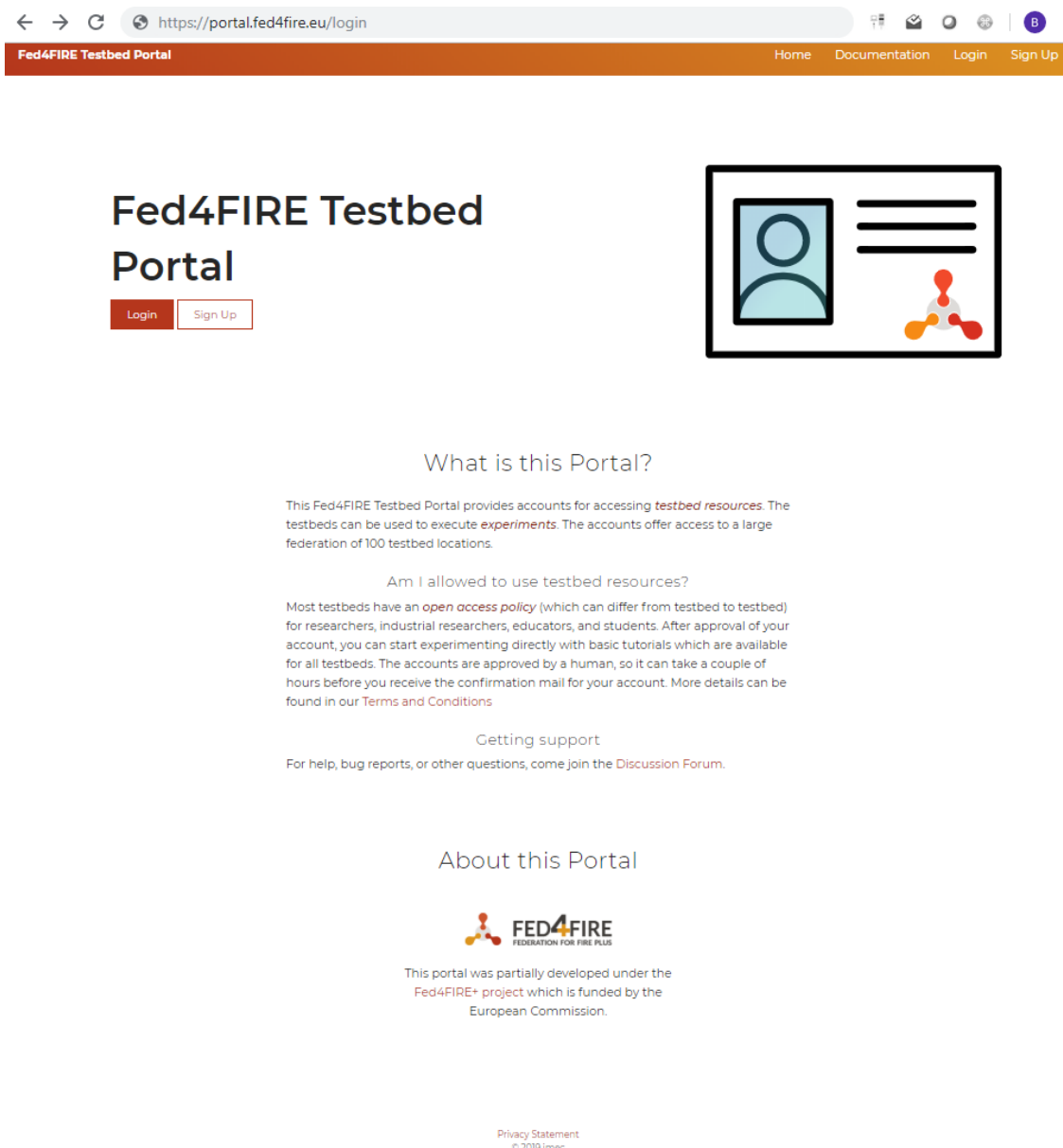
Table 2: Privacy Risks and Mitigation Measures

Privacy Risk	Initial mitigation recommendations	Implemented measures by testbeds
Missing end-to-end encryption: The traffic is transmitted without being encrypted	Adoption of encryption by default and by design.	SSH authentication is required to use the jFed tool, in principle no personal data is transmitted apart from the SSH key.
Use of unsecure or obsolete cypher suites: The traffic is encrypted, but the encryption methods have known vulnerabilities	Permanent review of the encryption methods.	Fed4Fire+ uses X.509 certificates for SSH authentication, updates will be introduced if vulnerabilities are detected
Man-in-the-middle attacks: Circumvention of mutual authentication between client and server by an attacker	Implementation of strong authentication and tamper detection mechanisms.	Individual SSH keys can be regenerated as necessary to ensure authentication. Personal data transfers are minimized by default to mitigate potential exploits by this attack
Missing transparency of service storage method: Data stored within a third-party- service may be leaked because the user has no control over storage security	Avoid use of third-party-services.	No third-party storage of personal data is carried out in Fed4Fire+.
Security vulnerabilities in service backend: The backend deployed by a service provider may be susceptible to security vulnerabilities	Scheduled and continuous testing and updating of all backend elements.	All the backends used in the framework of Fed4Fire+ are maintained by members of the consortium, particularly testbed owners. Their platforms are independently tested and updated.
Traffic analysis: Information is leaked and exploited through passive eavesdropping and analysis of encrypted transmission	Encryption of both metadata and packet data and routing under trusted third parties.	At a project-wide level, only the SSH keys are transmitted in the course of a normal Fed4Fire+ experiment. Communications between the testbeds are encrypted.
DNS request leakage: Secure DNS is not used and DNS requests are visible to everyone	Adoption of Secure DNS by default and by design.	Secure DNS has been introduced in the project

2.9 FED4FIRE EXPERIMENTERS AND PRIVACY STATEMENTS

2.9.1 Fed4FIRE account

When the user wants to create an account, he opens the Fed4FIRE portal (<https://portal.fed4fire.eu>), running on a server provided and maintained by imec, running in an imec datacenter in Gent, Belgium. The bottom of this site has a link to the imec privacy statement (<https://www.imec-int.com/en/privacy-statement>) (Figure 2).



← → ↻ 🔍 <https://portal.fed4fire.eu/login> 📄 📧 🌐 🌐 🌐 🌐 🌐

Fed4FIRE Testbed Portal Home Documentation Login Sign Up

Fed4FIRE Testbed Portal

Login Sign Up

What is this Portal?

This Fed4FIRE Testbed Portal provides accounts for accessing *testbed resources*. The testbeds can be used to execute *experiments*. The accounts offer access to a large federation of 100 testbed locations.


Am I allowed to use testbed resources?

Most testbeds have an *open access policy* (which can differ from testbed to testbed) for researchers, industrial researchers, educators, and students. After approval of your account, you can start experimenting directly with basic tutorials which are available for all testbeds. The accounts are approved by a human, so it can take a couple of hours before you receive the confirmation mail for your account. More details can be found in our [Terms and Conditions](#)

Getting support

For help, bug reports, or other questions, come join the [Discussion Forum](#).

About this Portal

 **FED4FIRE**
FEDERATION FOR FIRE PLUS

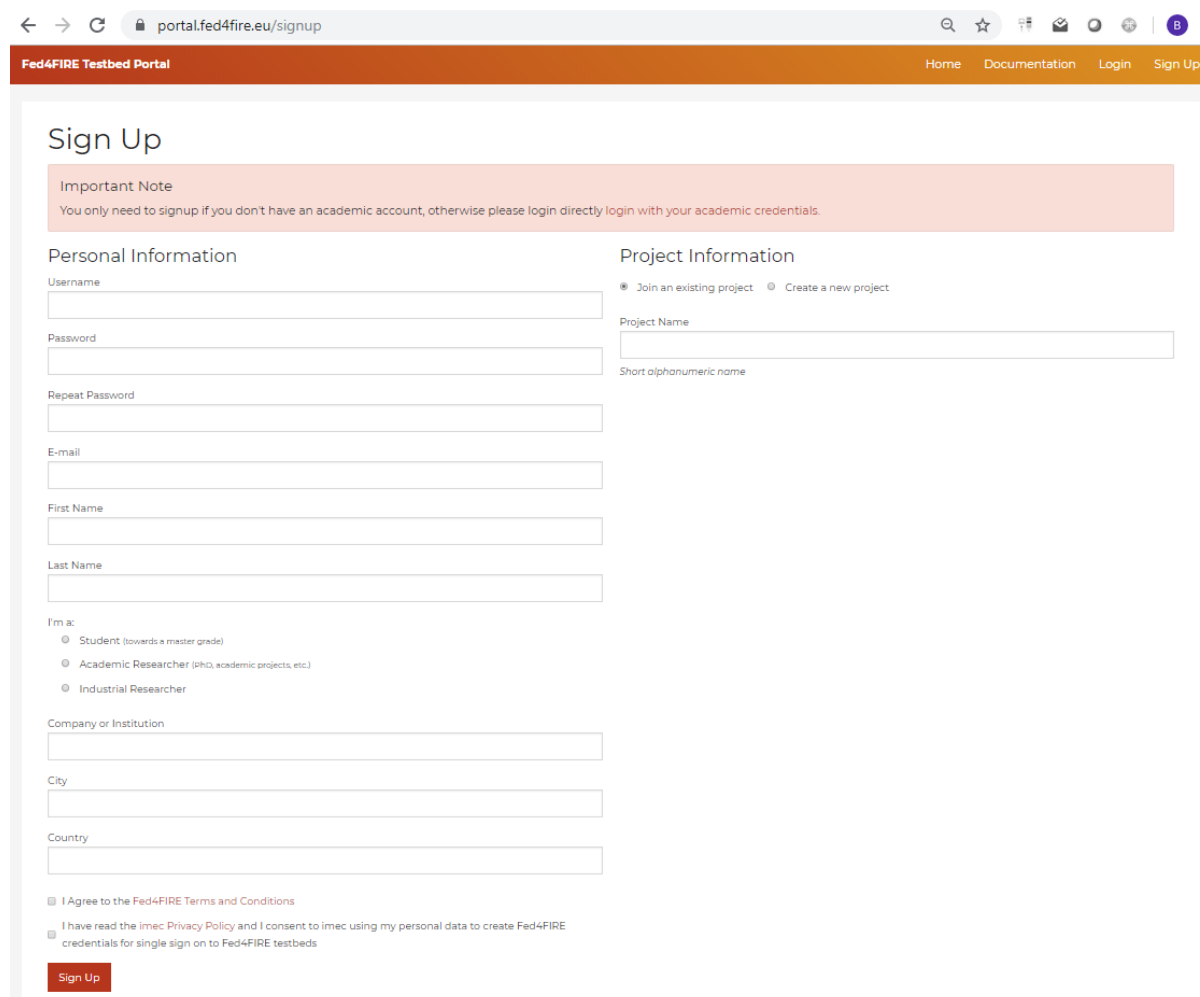
This portal was partially developed under the Fed4FIRE+ project which is funded by the European Commission.

[Privacy Statement](#)
© 2019 imec

Figure 2: Screenshot Fed4FIRE+ portal – Indication link to privacy statement

Apart from the privacy statement, there are also Fed4FIRE Terms and Conditions (<https://www.fed4fire.eu/terms/>) to inform the user about what constitutes acceptable and permitted use of testbed resources and tools (hereinafter ‘the Platform’) in the Fed4FIRE+ federation.

The terms and conditions and privacy statement have to be approved when signing up for an account, see screenshot of the sign-up form (this shows also the personal information that is asked) (Figure 3).



portal.fed4fire.eu/signup

Fed4FIRE Testbed Portal Home Documentation Login Sign Up

Sign Up

Important Note
You only need to sign up if you don't have an academic account, otherwise please login directly with your academic credentials.

Personal Information

Username

Password

Repeat Password

E-mail

First Name

Last Name

I'm a:

- Student (towards a master grade)
- Academic Researcher (PhD, academic projects, etc.)
- Industrial Researcher

Company or Institution

City

Country

I Agree to the Fed4FIRE Terms and Conditions

I have read the imec Privacy Policy and I consent to imec using my personal data to create Fed4FIRE credentials for single sign on to Fed4FIRE testbeds

Project Information

Join an existing project Create a new project

Project Name

Short alphanumeric name

Figure 3: Screenshot Fed4FIRE+ portal – Requirement for approval of terms and conditions and privacy statement

2.9.2 Fed4FIRE experiments on testbeds

Apart from the account on the central portal, experimenters also share personal information (their name and email address) with a testbed when they use this testbed. The jFed tool (running on the computer of the experimenter) sends the Fed4FIRE certificate to that specific testbed they want to use (the portal is not sending this information).

For this, jFed warns the experimenter (Figure 4), if the experimenter has not agreed with the specific terms and conditions and privacy terms of the testbeds he/she wants to use.

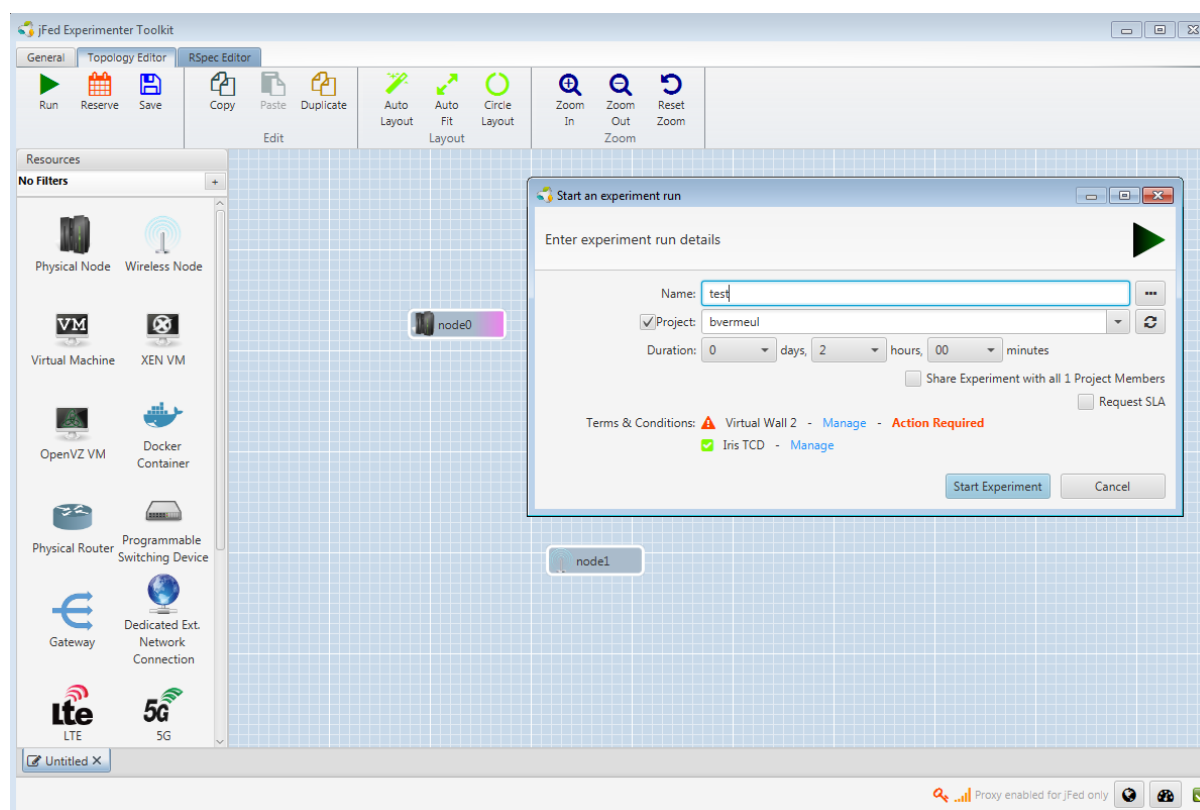


Figure 4: Warning by jFed if user has not agreed with terms and conditions and privacy terms of the testbeds he/she wants to use

The testbed specific terms and conditions and privacy statements are maintained and hosted by the specific testbeds. See below (Figure 5) for an example of the IRIS testbed policy. jFed opens that specific page (per testbed) so the user can read and accept this. The testbed can decide for how long an accepted privacy statement is valid, and oblige e.g. to re-sign every 6 months (or when it has changed).

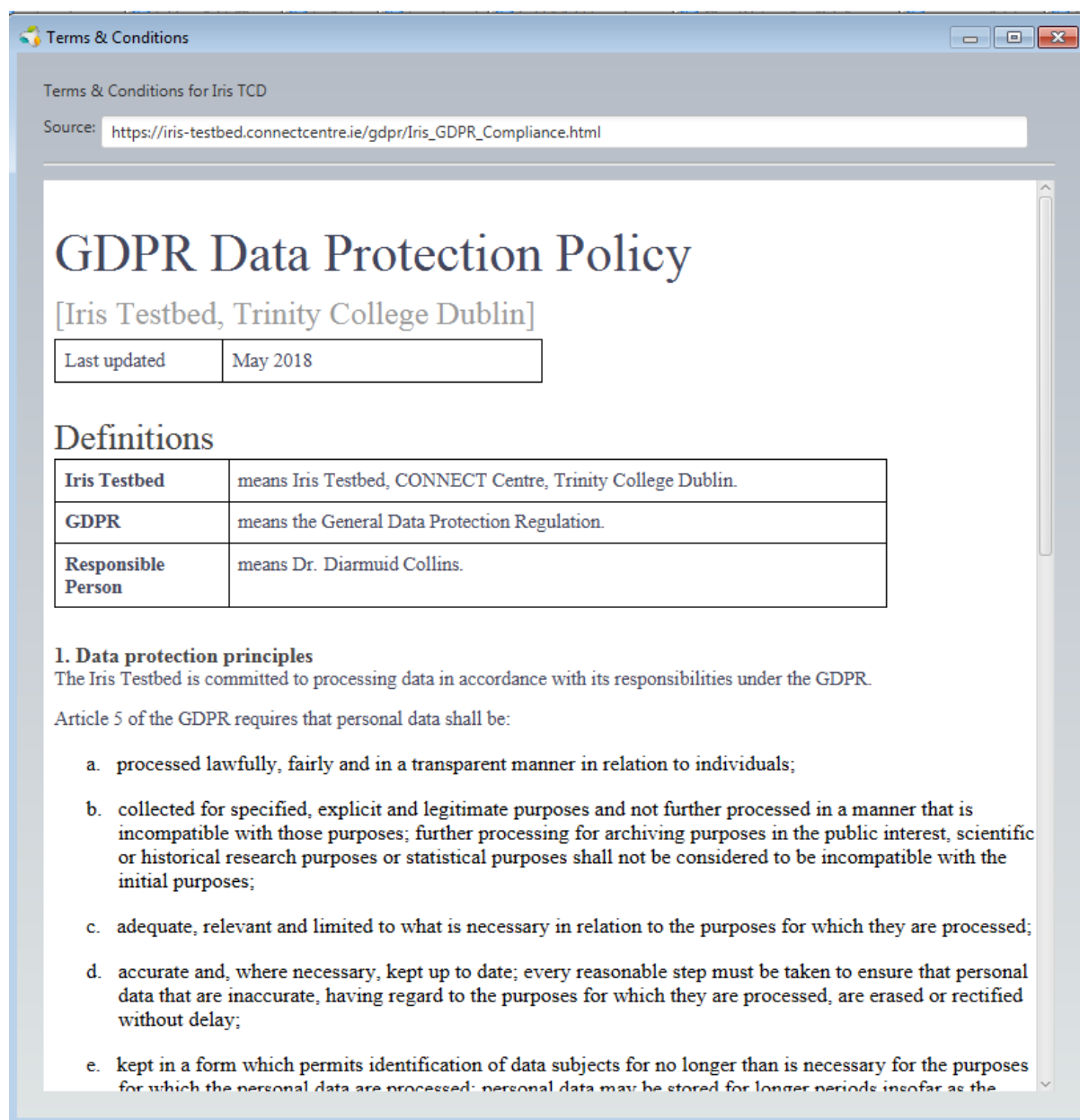


Figure 5: Testbed specific terms and conditions and privacy statements are maintained and hosted by the specific testbeds (example of the IRIS testbed policy)

2.9.3 Examples of experiments with personal data

Apart from the testbeds processing (minimum) personal data of its users, an experimenter can also process personal data in his/her experiment. Two examples:

- The experimenter can copy data (e.g. medical image datasets) to the testbed nodes to process
- The experimenter can collect personal data via the testbed (e.g. sniff mac addresses and moving mobile devices in a city testbed)

The testbed itself cannot know this, so the specific testbed policy needs to contain, if relevant, a section on this (the testbed is the data processor in this case while the experimenter is the data controller).

2.10 CONCLUSION

Personal data within Fed4FIRE+ is in two main forms:

1. Registration information of experimenters; and
2. Any personal data within an experiment.

The first of these scenarios is the domain of Fed4FIRE+ and GDPR measures are in place to manage this data. Fed4FIRE+ operates a portal where users can register. Fed4FIRE itself is not a legal entity (at this moment at least), so the portal's legal entity is imec, as the portal is running on imec's premises and maintained by imec personnel. The privacy policy presented to users at registration time is imec's. In addition, because of the federation model of testbeds with a central authority to create accounts, multiple levels of terms and conditions and privacy statements are implemented in Fed4FIRE, its tools and its testbeds.

In the second of these scenarios, personal data in the experiment is explicitly the responsibility of the experimenter, who acts as Data Controller for the personal data in their experiment, but Fed4FIRE+ will provide support experimenters (e.g. training and guidance) so that they may confidently manage the personal data in their experiment. Where an experiment contains personal data, the testbeds upon which the experimenter runs are deemed Data Processors, under the control of the experimenter in their role as Data Controller.

A Data Protection Officer network (DPO network) has been established comprising all major actors within Fed4FIRE+ who have a real or potential need to process personal data, and this is run by Mandat International, who is the project's Data Protection Officer. This DPO network functions as a knowledge sharing and support network that aims to help its members understand the requirements of data protection and to comply with relevant regulations such as the GDPR.

3 OPEN RESEARCH DATA

This deliverable follows directly on from D2.1 regarding Open Research Data (ORD), and this section's primary function is to report on the implementation and take-up of the ORD implementation plans reported in D2.1 and the support offered by Fed4FIRE+ for ORD.

3.1 INTEGRATION OF OPEN RESEARCH DATA INTO OPEN CALLS

Support for ORD in Fed4FIRE+ began from the third Open Call (OC3), which opened in October 2017. From this point going forward, experimenters have been encouraged (but crucially not forced, in line with the principle of *"as open as possible, as closed as necessary"*) and supported in Fed4FIRE+ to create ORD from their experiment results.

The primary form of support provided is via integration with the standard processes Fed4FIRE+ provides for Open Call management. The Open Calls each have documents that describe the call, a proposal template that serves as the application form, and if the proposal is successful, an agreement between the experimenter and IMEC. Once the experiment is complete, the experimenter is required to write a report. These documents are included in this deliverable as appendices, but in summary, they have been updated as follows to enable ORD to be supported.

- ➔ The Open Call Information document (Appendix 1) describes general information for prospective experimenters as well as eligibility criteria, rules and process for applications, and details specific to a particular Open Call, such as its rationale, funding & timings. The Information document has been extended with a dedicated section on Open Research Data. This describes the rationale behind ORD support and emphasises the key principle that ORD is encouraged but not mandated. It describes the process for and provides instructions on how to incorporate ORD in an experiment. This process was described in D2.1, and gives the experimenter multiple opportunities to opt in and out of ORD at the beginning and end of their experiment – at the beginning, an opt-in to ORD is not binding and the final decision to opt in or out of ORD is at the end of the experiment, because the experimenter may find results during their experiment that they wish to keep secret (e.g. a discovery that is commercially exploitable).
- ➔ The Experiment Proposal Template (Appendix 2, Section J) is filled in by prospective experimenters responding to an Open Call. The template has been updated to allow the experimenter to record their initial decision regarding ORD before the experiment begins. If the experimenter decides to opt-in, they need to fill in an Initial Data Management Plan (DMP) template. This was described in D2.1 and is intended to encourage the experimenter to think about the practicalities and implications of opening their experiment data, in the context of the FAIR principles⁴ (findable, accessible, interoperable and reproducible).
- ➔ The Experiment Report Template (Appendix 3, Section C) is completed by the experimenter once they have completed their experiment. The template has been updated to include the final decision whether to open or close data, as well as the template Final Data Management Plan. In addition, instructions on how to prepare a data package and upload it to Fed4FIRE+'s chosen archival repository, Zenodo. At this stage, the experimenter makes the final decision whether to open data or keep it closed. If they decide to keep it closed, they need to provide a

⁴ FAIR is an acronym for "findable, accessible, interoperable and reusable". See: Wilkinson, Mark D., Michel Dumontier, IJsbrand Jan Aalbersberg, Gabrielle Appleton, Myles Axton, Arie Baak, Niklas Blomberg et al. "The FAIR Guiding Principles for scientific data management and stewardship." *Scientific data* 3 (2016). <http://dx.doi.org/10.1038/sdata.2016.18>



reason. If the experimenter decides to open their results, they need to fill in the Final DMP and upload the data to Fed4FIRE+'s chosen archival repository, Zenodo. Zenodo issues a DOI for the data, and upon receipt of the DOI for the dataset, the costs claimed by the experimenter for preparation and upload of the data package are released to them.

3.2 ORD TAKE-UP IN OPEN CALLS

The following discussion covers the period from the opening of OC3 (October 2017), which was the first open call to incorporate ORD support, to the time of writing (June / July 2019 and updated in Oct 2019). This time period included OC3, OC4, OC5 and OC6. As of October 2019, OC3 and OC4 are totally complete – all experiments are finished and their experiment reports have been submitted. Most of OC5 experiments are still running, and OC6 experiments have just started.

In these calls, a total of 112 experiment proposals have been submitted to Fed4FIRE+, of which 92 opted for open data in their initial proposals – 82%. Of those that elected not to open data, all but one was either industrial or SME organisations, the remaining one being academia and the reasons given for opting out all amounted to commercial confidentiality.

To date, a total of 15 experiments have completed on Fed4FIRE+, and of these, 11 have created datasets, uploaded them to Zenodo and completed the final Data Management Plan (DMP).

3.2.1 Open Call 3

Open Call 3 applications for proposals opened on 18 October 2017 and closed on 15 January 2018. A breakdown of the statistics regarding ORD in OC3 is shown in Figure 6.

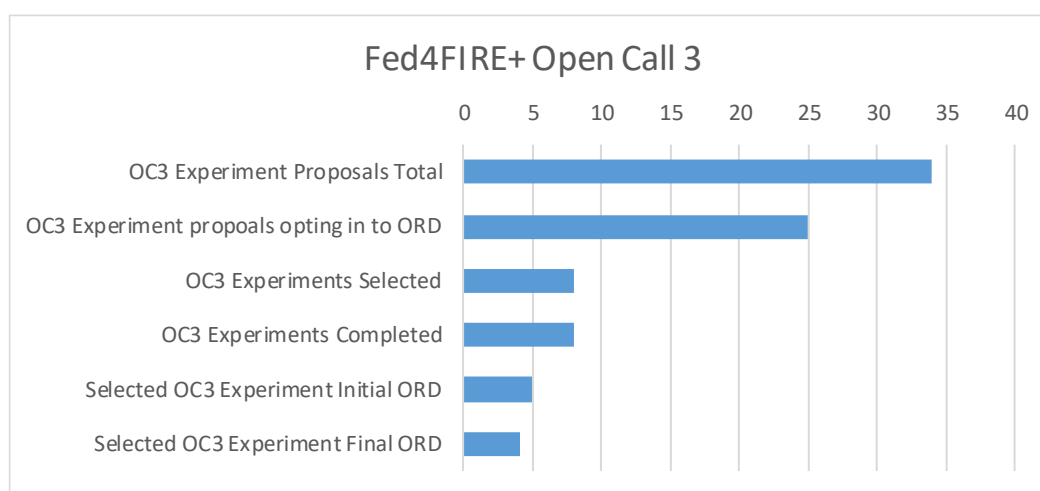


Figure 6: OC3 Open Research Data Take-Up

The top two bars represent the total number of applicants for OC3 (34), and the subset of this number who opted into ORD (25) – 74%.

The lower four bars represent the proposals selected for funding. The third bar indicates how many were selected (8) and the fourth bar represents how many are complete (also 8 – all are finished). The fifth and sixth bars represent the subset of the funded experiments who opted into ORD before the experiment (5), and those that remained opted in to ORD when the experiment finished, uploaded a dataset to Zenodo and completed the final DMP table. Of the five funded experiments who opted into ORD, four have completed a final Data Management Plan and uploaded their data to Zenodo, and one

D2.06 Updated Guidelines on Data Management



has opted out of ORD, citing commercial confidentiality. The following table shows the DOIs of the uploaded datasets together with their views and download statistics at the time of updating.

Call	Name	Initial ORD	Final ORD	DOI / Comment	Views 2019-10-28	DL 2019-10-28
F4Fp-03-L04	SODA	Yes		https://zenodo.org/record/3472626	11	1
F4Fp-03-L05	SIMBED	Yes	Yes	http://doi.org/10.5281/zenodo.2634272	36	2
F4Fp-03-L06	MAGIC	No	N/A	Opt out at proposal stage - commercial confidentiality	N/A	N/A
F4Fp-03-M13	IntelligentNFVscaler	Yes	Yes	http://doi.org/10.5281/zenodo.1476154	18	6
F4Fp-03-M14	ERASER	Yes	Yes	http://doi.org/10.5281/zenodo.1420391	80	70
F4Fp-03-M15	Fed4QoE	Yes	No	Opt out at experiment completion - commercial confidentiality	N/A	N/A
F4Fp-03-M20	DataTwin	No	N/A	Opt out at proposal stage - commercial confidentiality	N/A	N/A
F4Fp-03-M23	PiAS	No	N/A	Opt out at proposal stage - commercial confidentiality	N/A	N/A



3.2.2 Open Call 4

Open Call 4 applications for proposals opened on 18 June 2018 and closed on 18 September 2018. A breakdown of the statistics for OC4 is shown in Figure 7.

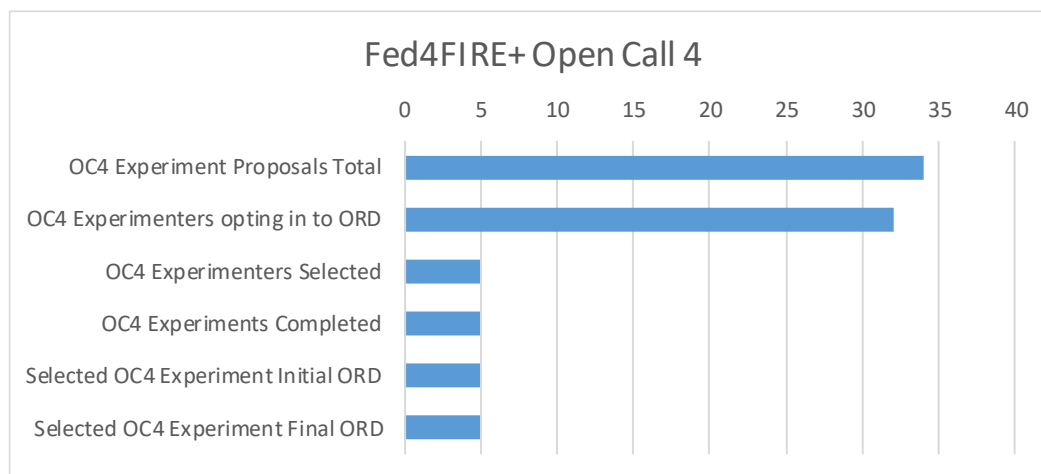


Figure 7: OC4 ORD Statistics

Of the 34 experiment proposals in OC4, 32 opted into ORD (94%). All of the five experiments selected were amongst those opting into ORD. All experiments are complete, and all opted into ORD, have completed the final DMP table and uploaded the data to Zenodo.

Call	Name	Initial ORD	Final ORD	DOI	Views 2019-10-28	DL 2019-10-28
F4Fp-04-M08	IIoT-REPLAN	Yes	Yes	http://doi.org/10.5281/zenodo.3366025	14	32
F4FP-04-M15	ANGEL	Yes	Yes	http://doi.org/10.5281/zenodo.3269936	24	5
F4FP-04-M25	FB-FIRE	Yes	Yes	http://doi.org/10.5281/zenodo.3368599	5	2
F4Fp-04-M27	UNIC	Yes	Yes	http://doi.org/10.5281/zenodo.3356734	8	3
F4FP-04-M30	SUNSeT	Yes	Yes	http://doi.org/10.5281/zenodo.3241458	4	5



3.2.3 Open Call 5

Open Call 5 applications for proposals opened on 21 December 2018 and closed on 26 March 2019.

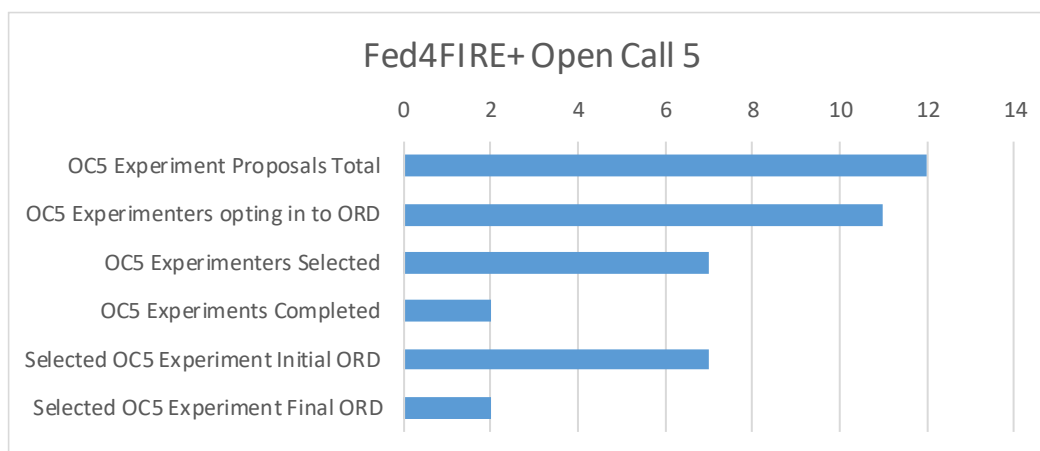


Figure 8: OC5 ORD Statistics

12 experiment proposals were submitted to OC5 and 11 opted into ORD (92%). 7 experiments were selected for funding and all of these were amongst those who opted into ORD. At the time of updating this report (Oct 2019), two experiments have completed. Both of these have remained opted into ORD, have created their final DMP and uploaded datasets to Zenodo.

Call	Name	Initial ORD	Final ORD	DOI / Comment	Views 2019-10-28	DL 2019-10-28
F4Fp-05-L02	AdaHon	Yes		Experiment not complete		
F4Fp-05-L04	SIMBED+	Yes		Experiment not complete		
F4Fp-05-M02	SCION on Fed4FIRE+	Yes		Experiment not complete		
F4Fp-05-M04	DYNAMO	Yes	Yes	http://doi.org/10.5281/zenodo.3483996	2	1
F4Fp-05-M06-STS	Internet on FIRE	Yes		Experiment not complete		
F4Fp-05-M07	CDN-X-ALL	Yes	Yes	http://doi.org/10.5281/zenodo.3457936 http://doi.org/10.5281/zenodo.3459164	42	2
F4Fp-05-M08	QoS Predictions WSN	Yes		Experiment not complete		



3.2.4 Open Call 6

Open Call 6 applications for proposals opened on 12 June 2019 and closed on 10 Sept 2019.

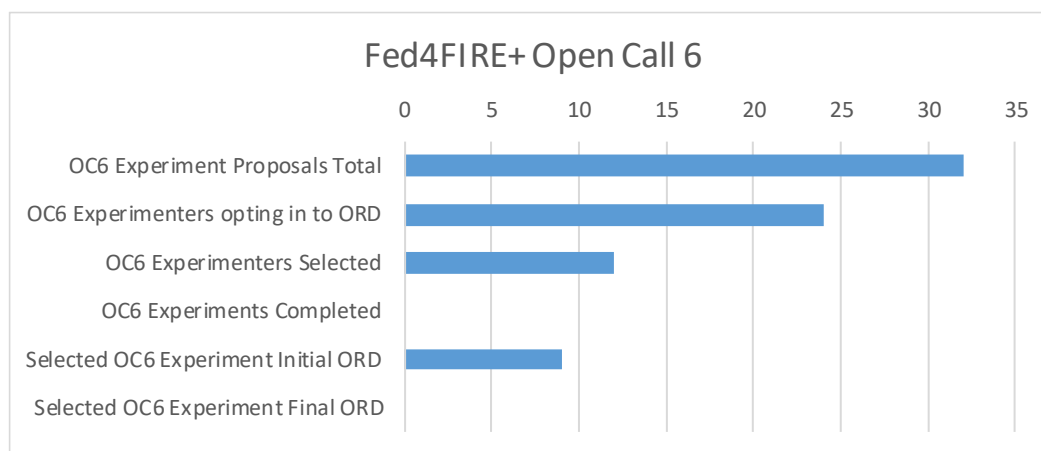


Figure 9: OC6 ORD Statistics

32 experiment proposals were submitted to OC5 and 24 opted into ORD (75%). 12 experiments were selected for funding 9 amongst these opted into ORD. Of those that opted out, all cited commercial confidentiality, all are SMEs (two have previous participation in the SME-only continuous call). At the time of updating this report (Oct 2019), no experiments have completed.

Call	Name	Initial ORD	Final ORD	DOI / Comment	Views 2019-10-28	DL 2019-10-28
F4Fp-06-M01-Stage 2 SME	Lucy	Yes		Experiment not complete		
F4Fp-06-M11-Stage 2 SME	Fed4AI-Stage2	No		Experiment not complete		
F4Fp-06-M19-Stage 2 SME	WRIO Internet OS	Yes		Experiment not complete		
F4Fp-06-M21-Stage 2 SME	DRAFT	Yes		Experiment not complete		
F4Fp-06-M23-Stage 2 SME	CoPro5G	Yes		Experiment not complete		
F4Fp-06-M25	MOTIVE	Yes		Experiment not complete		
F4Fp-06-M28	Smart IoT deployment	No		Experiment not complete		
F4Fp-06-M29-Stage 2 SME	Wi-Fi HaLow eva	No		Experiment not complete		
F4Fp-06-M30	MECinFIRE	Yes		Experiment not complete		
F4Fp-06-M31	MECPerf	Yes		Experiment not complete		



F4Fp-06-M33	srsV2X	Yes		Experiment not complete		
F4Fp-06-M34-Stage 2 SME	CityScan	Yes		Experiment not complete		

3.2.5 Continuous SME Call

The continuous SME call is different from other Open Calls: it is restricted to SMEs, it is open all the time, applications are lightweight, applications are assessed and responded to quickly experiments are small and the funding amounts are low (typically less than EUR 12500). These types of experiment are not traditionally expected to be good candidates for ORD, considering the small scale of the experiments and that the call is directly targeted at SMEs, commercial organisations who have strong needs for commercial confidentiality. As a result, it has been decided that ORD incentives will not be offered in the Continuous SME call, but should experimenters in this call be keen to create and upload ORD, support will be given. Some experimenters in the Continuous SME call go on to regular open calls for more in-depth experiments, and these experiments will be treated as any other in terms of ORD encouragement and support.

3.3 RISK ANALYSIS OF LONG-TERM STORAGE OF OPEN RESEARCH DATA

The original Fed4FIRE+ DOA specified assessments of the risks and costs of long-term data storage:

“Fed4FIRE+ will also address two key concerns of data management over the long term: risk management and evaluation of the costs versus the benefits of data retention. Retention and access to research data should consider risks of data loss resulting from factors such as technical obsolescence, hardware failures, under investment etc., so the DMP will incorporate approaches for, and results of, risk analyses, building on previous work in FP7 DAVID but specifically applied to the specific context of FIRE research data retention workflows and scenarios. A further key concern of organisations hosting their own research data repository is to determine the costs of storing the data long term, and to evaluate these costs against the benefits of the long-term data retention. To address cost questions of long-term research data storage, the DMP will build on work in FP7 BonFIRE to provide strategies and techniques to evaluate the cost of storage and optimise the utility of the storage while keeping costs to a minimum.”

However, based on the analysis conducted in D2.1, there is no need for further work regarding the risks and costs of long-term retention of Open Research Data, beyond what has already been undertaken and reported in D2.1. The reason for this is because of the decision to select a third-party archival repository, Zenodo (<https://zenodo.org/>), rather than go to the unnecessary expense of creating our own repository in Fed4FIRE+.

Risk and cost assessments were undertaken in Fed4FIRE+ D2.1, Initial Guidelines on Data Management and concluded that the decision to choose Zenodo mitigated the major risks of long-term retention of ORD. The reasons for choosing Zenodo are given in detail in Fed4FIRE+ D2.1, but they are summarised below:

- ➔ Zenodo is hosted by CERN, so it is unlikely to disappear any time soon, and has a stated long-term data preservation policy.
- ➔ Zenodo exports descriptive metadata to ORD search engines, enabling the data to be easily found.
- ➔ Zenodo is an issuer of Digital Object Identifiers (DOIs)⁵, enabling the data to be uniquely identified.
- ➔ Zenodo is flexible on licensing of data.
- ➔ Zenodo provides automated reporting to the EC for open data stored within it, so evidence of the commitment from Fed4FIRE+ and experimenters to provide open experiment data can be easily verified.

The main risks to ORD are whether there are questions over the long-term survival of the data repository in which the ORD are stored and its guarantees against data loss or compromise. Zenodo is operated by CERN, which is a large organisation with funding for at least 20 years, so the chances of Zenodo disappearing are low. Zenodo also has a vested interest in the security and integrity of its data and naturally operates high availability & backups to ensure access to the data. Zenodo also hashes the data to prevent compromise or tampering.

In Zenodo, the costs to the experimenter (for reasonable amounts of data) are zero for storage. The remaining costs to the experimenter are the time in the preparation of a data package for upload to the repository. As an encouragement to experimenters to support ORD, Fed4FIRE+ will cover their legitimate ORD data preparation costs up to EUR 500. In addition, Fed4FIRE+ provides support to experimenters to help them create their data packages and upload them to Zenodo (although support has been rarely needed as the process is not challenging).

Because of the decision to use Zenodo and given the reasons above, a contract amendment has been proposed to migrate the task on risk and cost assessment of long-term data storage to other equally useful work, and this is described next.

⁵ <https://www.doi.org/>

3.4 PROPOSAL FOR CONTRACT AMENDMENT – GDPR DECISION SUPPORT FOR EXPERIMENTATION PLATFORMS

Because there is no need for additional risk analysis of long-term ORD storage as described above, it is proposed to replace the risk analysis work with investigations into decision support for GDPR compliance in experimentation facilities, namely the testbeds currently within Fed4FIRE+ and especially new testbeds who may join in the future. The proposed work is aimed to benefit the testbeds involved in Fed4IRE+ experiments in that they can assess their compliance to the GDPR, as well as experimenters, who can understand the GDPR-specific risks of running an experiment over one or more testbeds. As such, this proposal supports the two cases of personal data processing within Fed4FIRE+ described in section **Error! Reference source not found.** above. This proposal has been included in the July 2019 Fed4FIRE+ Contract Amendment, and details of the proposal are as follows.

Fed4FIRE+ already has GDPR expertise in T2.7, and the proposed extension is concerned with providing semi-automated decision support concerning GDPR compliance targeted at the specific scenarios relevant to Fed4FIRE+, which will utilise this expertise encoded into a decision support system that will enable the expertise to be distributed at lower cost and at a wider scale than when it is provided as consultancy by human experts. Fed4FIRE+ will achieve this by enhancing IT Innovation's "System Security Modeller" (SSM) tool to extend assessment of GDPR compliance in human-IT systems to the situations found in Fed4FIRE+, which are often multi-stakeholder, in that an experiment is run across multiple testbeds.

This approach is founded in a risk assessment methodology developed over the course of seven years at IT Innovation. Work done in the FP7 OPTET (Operational Trustworthiness Enabling Technologies) project used a multi-disciplinary and integrated approach to identify and address understanding of risk within internet-based socio-technical systems and its impact on the trustworthiness of those systems^{6, 7, 8}. H2020 5G-ENSURE and RESTASSURED built on this work to develop a risk assessment framework that analyses threats and associated trust relationships, which has specifically been applied in communication network situations⁹. The framework is based on an asset-centric approach, where assets and their interconnections in the system under evaluation are specified and a knowledge base determines threats associated with each asset. So-called "controls" (also from the knowledge base) can be applied to the assets that can mitigate the threats and thus increase or restore the trustworthiness of an asset under threat and its impact on the overall system. Users supply input on the impact of "misbehaviours" that can be caused by threats, and the SSM tool calculates the risk level from each threat it has identified, taking account of the controls that have been specified.

Crucially, the framework supports modelling of socio-technical systems, including typical IT assets such as servers and networks but also humans, roles, organisations and potentially more general concepts such as communities and values. Assets can be combined into networks that form the basis of scenarios where the overall risk to different actors can be assessed. In H2020 SHIELD and RESTASSURED, IT Innovation is currently investigating the use of asset, threat and risk-based

⁶ Ajay Chakravarthy, Xiaoyu Chen, Bassem Nasser, and Michael Surridge. 2015. Trustworthy systems design using semantic risk modelling. (February 2015). <https://eprints.soton.ac.uk/383465/>

⁷ Nazila Gol Mohammadi et al. 2014. Maintaining Trustworthiness of Socio-Technical Systems at Run-Time. In Trust, Privacy, and Security in Digital Business. Cham, 1–12.

⁸ Nazila Gol Mohammadi et al. 2015. Combining Risk-Management and Computational Approaches for Trustworthiness Evaluation of Socio-Technical Systems. In Proceedings of CAiSE 2015. 237–244.

⁹ Mike Surridge, Gianluca Correndo, Ken Meacham, Juri Papay, Stephen C. Phillips, Stefanie Wiegand, and Toby Wilkinson. 2018. Trust Modelling in 5G mobile networks. In Proceedings of the 2018 Workshop on Security in Softwarized Networks: Prospects and Challenges (SecSoN '18). ACM, New York, NY, USA, 14-19. DOI: <https://doi.org/10.1145/3229616.3229621>



techniques to model regulatory compliance by considering the absence of compliance to a regulatory requirement as a threat, and the mechanisms possible to enable compliance as mitigations to that threat. The initial experiments in this investigation are using the GDPR as an exemplary regulation to determine the issues and requirements for extending the asset and risk-based modelling work towards regulatory compliance decision support.

The proposal for Fed4FIRE+ is to determine how to build on this approach to provide decision support for the assessment of GDPR compliance in human-IT systems with a special attention applied to experimentation platforms (e.g. Fed4FIRE+'s testbeds) and considering the situation where experiments are run across multiple testbeds, which gives rise to different controller-processor relationships and also poses questions regarding whether the experimenter or a testbed can be a controller or a processor. Fed4FIRE+ will investigate these implications on GDPR compliance and the respective roles played by different stakeholders with their associated obligations in the cases and scenarios faced by experimenters and testbeds within Fed4FIRE+. The scenarios described in Section 2 will provide the contexts for and inform these case-based investigations.

4 CONCLUSIONS & NEXT STEPS

This deliverable has reported on the data aspects of Fed4FIRE+ in two significant ways: via Fed4FIRE+'s support for Data Protection in the form of its implementation of GDPR aspects, and Fed4FIRE+'s support for the EC's Open Research Data initiative.

A DPO (Data Protection Officer) Network has been established within Fed4FIRE+ consisting of the Project DPO (Mandat International) and individual testbeds' DPOs. The network's purpose is to provide a community and support for the testbed DPOs in dealing with data protection issues.

There are two types of personal data relevant to Fed4FIRE+:

1. Registration and login details of experimenters. Fed4FIRE+ operates an identity provider, run by IMEC, which is the controller and collector of this information, and so IMEC's DPO is responsible for this personal information.
2. Personal information included in the data used within an experiment. Here, we assert that the responsibility for this data is with the experimenter, since they designed the experiment and are therefore deemed to be the Data Controller for the experiment, with the testbeds the experiment runs on identified as Data Processors under the control of the experimenter. It is critically acknowledged that the experimenters need support to confidently undertake the responsibilities of Data Controllers, so an item of further work is for Fed4FIRE+ to help these actors to process experiments containing personal data legally and fairly, respecting the rights of the data subjects via training and guidance.

For Open Research Data, the major conclusion is that the ORD policies and programme integrated with the Open Calls is by and large successful, in that the process is working and opt-in to ORD is strong. At the time of writing, the first results have been prepared and uploaded to the Fed4FIRE+ chosen repository, Zenodo. Future deliverables will provide updated statistics on the continued uptake of ORD in Fed4FIRE+.

Because of the choice of an external ORD storage repository that is well-known, robust and has a long-term chance of survival that is free of charge at the point of use, it has been decided that to conduct risk and cost assessments of long-term data storage is not necessary, and we have proposed an update to the DOA in the July 2019 contract amendment in which this work is removed and replaced by investigations into decision support for GDPR compliance, specifically targeting the multi-stakeholder situations (e.g. an experiment run over multiple testbeds) faced within Fed4FIRE+. This proposed work will not only provide an efficient means to support the testbeds in Fed4FIRE+ but also especially new prospective testbeds wishing to join the federation.

Next steps include continued monitoring of the take-up for in Fed4FIRE+, answering requests for support and making any changes to the process or documentation needed as a result of these observations.

5 APPENDICES

5.1 OPEN CALL INFORMATION





3rd Fed4FIRE+ Open Call - Experiments

“Medium Experiments” & “Large Experiments”

Call information:

- Project full name: **Fed4FIRE+: Federation for FIRE**
- Project grant agreement number: **732638**
- Call identifier: **F4Fp-03**
- Call title: **3rd Fed4FIRE+ Competitive Call - Innovative Experiments Category “Medium Experiments” & “Large Experiments”**

Submission deadline 15 January 2018, at 17:00 Brussels local time

Call Objectives:

The major objective of this Call is to make Fed4FIRE’s federated infrastructure directly available for execution of innovative experiments by experimenters at both industrial (including SMEs) and research organisations. Examples of such experiments may include but are not limited to testing of new protocols or algorithms, performance measurements or scalability testing. These Calls envisage experiments by which existing products or services are tested, implemented or optimized on the Fed4FIRE+ testbeds rather than proposing or developing new ideas from scratch.

Funding for Experimenters:

Funding is available to support experimenters, as described in the following table.

Experiment Type	Max Experimenter Funding Per Experiment	Testbed Patron Funding per experiment	Max number of experiments funded in this call	Max duration of experiment
Medium	€ 55 000	€ 5000	5	6 months
Large	€ 95 000	€ 5000	2	12 months

Eligibility:

- Proposals will only be accepted from a single party eligible for participation in EC H2020-projects.
- Proposers must from parties or organisations that are not already part of the Fed4FIRE+ project consortium.
- Proposers can submit multiple experiment proposals, but only one experiment per proposer will be selected for funding in this Call.
- Proposers who have submitted proposals in previous calls of the Fed4FIRE+ - project (Open Call 01 and Open Call 02) are allowed to re-submit.

Detailed information about the open call and its aspects can be retrieved online (www.fed4fire.eu)

Language in which the proposal must be submitted: English

Contact: contact@fed4fire.eu

1 Table of Contents

1	Table of Contents	2
2	Introduction to Fed4FIRE+	3
3	Objectives of the call.....	4
4	Eligibility	5
5	Inclusion into the consortium	6
6	Participation in meetings and submission of reports	7
6.1	Submission of reports	7
6.2	Attendance at meetings.....	7
7	Targeted timing:.....	9
7.1	Medium Experiments.....	9
7.2	Large Experiments.....	9
8	Open Research Data	10
8.1	Motivation & Principles	10
8.2	Data Archive.....	10
8.3	Funding Available.....	11
8.4	Process	11
9	Proposal template.....	13
10	Support during experiment and the role of the Patron.....	15
11	Budget & Payment scheme.....	16
11.1	Compliance rules.....	16
11.2	Budget.....	16
11.3	Submission of invoices	16
12	Access to Foreground information from the project.....	17
13	Reporting.....	18
14	Criteria for evaluation and ranking of experiments.....	19

2 Introduction to Fed4FIRE+

Fed4FIRE+ is a Research and Innovation Action under the European Horizon 2020 Programme addressing the work programme topic Future Internet Research and Experimentation. The project started on 01 January 2017 and runs for 60 months, until the end of 2021.

The Fed4FIRE+ project has the objective to run and further improve Fed4FIRE+'s "best-in-town" federation of experimentation facilities for the Future Internet Research and Experimentation initiative. Federating a heterogeneous set of facilities covering technologies ranging from wireless, wired, cloud services and open flow, and making them accessible through common frameworks and tools suddenly opens new possibilities, supporting a broad range of experimenter communities covering a wide variety of Internet infrastructures, services and applications.

Fed4FIRE+ continuously upgrades and improves the facilities and include technical innovations, focused towards increased user satisfaction (user-friendly tools, privacy-oriented data management, testbed SLA and reputation, experiment reproducibility, service-level experiment orchestration, federation ontologies, etc.). It will open this federation to the whole community and beyond, for experimentation by industry and research organisations, through the organization of Open Calls and Open Access mechanisms

The project also offers a flexible, demand-driven framework which allows test facilities to join during the course of its lifetime by defining a set of entry requirements for new facilities to join and to comply with the federation.

Fed4FIRE+ also continues to build on the existing community of experimenters, testbeds and tool developers and bring them together regularly (two times a year) in engineering conferences to have maximal interaction between the different stakeholders involved.

An overview of the available FIRE facilities offered through Fed4FIRE+ can be retrieved at the [facility overview page on the Fed4FIRE+ website](#)¹. Additional background information about both the offered facilities, the tools adopted by the federation, and the implementation steps needed from a facility when joining the federation can also be found in [the Fed4FIRE+ training material](#)².

¹ <https://www.fed4fire.eu/testbeds/>

² <http://doc.fed4fire.eu/>

3 Objectives of the call

The major objective of this Open Calls is to make the federated infrastructure directly available for execution of innovative experiments by experimenters at both industrial (including SMEs) and research organisations. These experiments should be of a duration as defined by the type of the call (Extra Small, Small, Medium or Large) and use one or more Fed4FIRE+ testbeds. Examples of such experiments may include but are not limited to testing of new protocols or algorithms, performance measurements, service experiments. It is required that these experimenters will come from parties or organisations that are not part of the Fed4FIRE+ project consortium.

In view of the targeted timeline and duration of the experiment, it should be clear that these Calls envisage experiments by which existing products or services are tested, implemented or optimized on the Fed4FIRE+ testbeds rather than proposing or developing new ideas from scratch. Examples of such experiments may include but are not limited to testing of new protocols or algorithms, performance measurements, service experiments.

The Fed4FIRE+ project is issuing this series of open and competitive calls for experiments with a degree of industrial and/or scientific innovation, relevance for the Fed4FIRE+ federation and an appropriate scale of complexity. Independent evaluations of the submitted proposals will be performed, in order to select experiments which will be executed within the project. It is required that the experiments are performed by a single organization.

This 3rd Open Call targets 2 specific categories for experiments:

- “Medium Experiments” with a maximum budget (including the financial support to the Fed4FIRE+ partner(s) acting as a Patron) of € 60 000 and a maximum duration of 6 months.
- “Large Experiments” with a maximum budget (including the financial support to the Fed4FIRE+ partner(s) acting as a Patron) of € 100 000 and a maximum duration of 12 months.

The proposal template will allow ticking one and only one of these categories. The top ranked proposals in the category “Medium Experiments” with a maximum of 5 experiments and the top ranked proposals in the category “Large Experiments” with a maximum of 2 experiments will be selected for funding.

Benefits for an experimenter to propose experiments on the Fed4FIRE+ federation of testbeds:

- Possibility to perform experiments that break the boundaries of different testbeds or domains (wireless, 5G, wired, OpenFlow, cloud computing, smart cities, services, etc.)
- Easily access all the required resources with a single account.
- Focus on your core task of experimentation, instead of on practical aspects such as learning to work with different tools for each testbed, requesting accounts on each testbed separately, etc.
- An extra benefit which is offered in this call is the dedicated support from specific Fed4FIRE members. Each proposer, preparing a proposal is required to seek a supporting Fed4FIRE consortium partner or partners (the “Patron”) that will be in charge of dedicated (advanced) support of the experiment.

4 Eligibility

- Proposals will only be accepted from parties eligible for participation in EC H2020-projects.
- Proposals will only be accepted from single parties (no consortia are allowed).
- Proposers must from parties or organisations that are not already part of the Fed4FIRE+ project consortium.
- Proposers can submit multiple experiment proposals, but only one experiment per proposer will be selected for funding in this Call. In case multiple proposals are submitted by the same party, reference should be made to each submitted proposal and clear indication should be given on the complementarity of the proposals.
- Proposers who have submitted proposals in previous calls of the Fed4FIRE+ - project (Open Call 01 and Open Call 02) are allowed to re-submit. Details on how this information needs to be included in the proposal are given below and should be included in a specific section in the proposal (cfr. Proposal template)
 - Parties who have submitted proposals in previous calls which were NOT selected for funding should indicate the exact dates and details of the previous submissions.
 - Parties who have submitted proposals in previous calls which were selected for funding should indicate the difference between the current proposal and the previously submitted proposal.
 - Parties belonging to a legal entity of which other groups have submitted proposals in previous calls also need to indicate the difference between the current proposal and the previously submitted proposals.

5 Inclusion into the consortium

Once a party is selected to perform the proposed experiment, it will be contracted by the project coordinator (imec) as a 3rd Party receiving financial support. This will require the signature of the Agreement of which can be found as download on the Fed4FIRE+ website together with this Call information.

6 Participation in meetings and submission of reports

6.1 Submission of reports

(templates can be found as download on the Fed4FIRE+ website together with this Call information)

The proposer will need, if its experiment is:

- To submit a report at the end of the experiment using the template in Annex 2 to this document.
- To prepare a Poster (A1-format) describing the objective and results of the experiment as well as the impact of the experiment on the proposers' business. This poster can be used by the Fed4FIRE+ consortium at public events and will be used at the occasion of the review meetings.
- To prepare a flyer (2 A4-pages) describing the objective and results of the experiment as well as the impact of the experiment on the proposers' business. This flyer can be used by the Fed4FIRE+ consortium at public events.
- To prepare a presentation and demo explaining and illustrating:
 - the objective and results of the experiment
 - the impact of the experiment on the proposers' business.
 - The feedback towards the Fed4FIRE+ consortium on the use of the facilities
- The production of a short video about the experiment is recommended. This video will be used by the Fed4FIRE+ project at public events.

6.2 Attendance at meetings

- FEC3 (March 13-15, 2018): Paris, France:
 - To be attended by all selected experimenters
 - Objective: attend tutorials and learn about Fed4FIRE+
- FEC4 & Formal Review Meeting (October 2018): Belgium
 - To be attended by all finished experiments in the category "Medium Experiments"
 - To be attended by the running experiments in the category "Large Experiments"
 - Objective:
 - presentations by the finished and running experiments will serve as tutorials and demonstrations towards participants and new experiments attending the event.
 - finished experiments in the category "Medium Experiments" will undergo a formal review by the EC at this FEC4. This formal review is required for obtaining full payment of the experimenters.
- FEC5 (March/April 2019): TBD
 - To be attended by all finished experiments in the category "Large Experiments"
 - Objective:
 - presentations by the finished experiments will serve as tutorials and demonstrations towards participants and new experiments attending the event.
- Formal review meeting (Belgium)
 - A formal review meeting by EC representatives of all finished experiments will also be required. These formal review meetings will be organized according to the availability of the reviewers. At FEC4, a formal review will be possible for the

finished experiments in the category “Medium Experiments”. A formal review meeting will be organized for the finished experiments in the category “Large Experiments” at a date co-located with FEC5 or later.

- It is therefore recommended to budget these as separate meetings in the proposal.
- Project meetings
 - As the experimenter will be linked to the project as 3rd Party, there will no possibility to attend formal meetings of the consortium but specific (remote) meetings regarding the experiment can be set up with Fed4FIRE+ partners. The engineering conferences should be used to discuss face-to-face.

7 Targeted timing:

7.1 Medium Experiments

- Feasibility Check Deadline: 08 January 2018
(draft proposal to Fed4FIRE+ partner(s) acting as Patron)
- Submission deadline: 15 January 2018
- Targeted acknowledgment of selection: 15 February 2018
- Attending FEC3 Tutorials: 13-15 March 2018
- Start of the experiment: March 2018
- End of the experiment September 2018 (Medium Experiments)
(this includes the time needed for the final reporting)
- Submission of Report: September 2018 (Medium Experiments)
- Presentation at FEC4: October 2018 (Medium Experiments)
- Formal review at FEC4: October 2018 (Medium Experiments)

7.2 Large Experiments

- Feasibility Check Deadline: 08 January 2018
(draft proposal to Fed4FIRE+ partner(s) acting as Patron)
- Submission deadline: 15 January 2018
- Targeted acknowledgment of selection: 15 February 2018
- Attending FEC3 Tutorials: 13-15 March 2018
- Start of the experiment: March 2018
- Intermediate presentation at FEC4 October 2018 (Large Experiments)
- End of the experiment March 2019
(this includes the time needed for the final reporting)
- Submission of Report: March 2019
- Final Presentation at FEC5 or FEC6 Spring (FEC5) or Fall (FEC6) 2019
- Attendance of formal review: Fall 2019
(eventually co-located with either FEC6,
but to be budgeted as separate meeting)

8 Open Research Data

8.1 Motivation & Principles

In order to support open and repeatable scientific experiments, the EC is advocating that experimenters publish their experiment data^{3,4}. This is not mandatory: the EC recognises that there are legitimate reasons why experimenters may want to keep their data confidential. To support this in Fed4FIRE+, experimenters are encouraged (but not mandated) to create a data package containing their experiment results with all data that supports them, and upload it to the Fed4FIRE+ approved repository so that it may be found and reused by other interested parties.

The EC's guiding principle regarding open research data is "*AS OPEN AS POSSIBLE, AS CLOSED AS NECESSARY*". This means the default situation is that all experiment data should be open but if there are genuine reasons why experiment data is not to be opened, experimenters can opt out and their experiment data can be kept confidential. Fed4FIRE+ experimenters can opt out of opening data at any time up to the point of publication after the experiment has completed, even if they have previously declared that they want to open data. Experiment proposers need to state the reasons why they will not open data, and these can include:

- Commercial confidentiality & IPR
- Personal data
- Conflict with the experiment's main objective

In general, most academic experimenters are anticipated to want to open data in order to support their academic work, and most commercial experimenters will want to keep their data confidential, but the final decision is the experimenter's, provided they give valid reasons for opting out of opening data.

8.2 Data Archive

The repository chosen for Fed4FIRE+ is **Zenodo**⁵. The reasons for this choice are given in detail in Fed4FIRE+ D2.1, Initial Guidelines on Data Management, but they are summarised here:

- Zenodo is hosted by CERN, so it is unlikely to disappear any time soon, and has a stated long-term data preservation policy.
- Zenodo exports descriptive metadata to ORD search engines, enabling the data to be easily found.
- Zenodo is an issuer of Digital Object Identifiers (DOIs)⁶, enabling the data to be uniquely identified.
- Zenodo is flexible on licensing of data.

³ https://ec.europa.eu/research/press/2016/pdf/opendata-infographic_072016.pdf

⁴ http://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-data-mgt_en.pdf

⁵ <https://zenodo.org/>

⁶ <https://www.doi.org/>

- Zenodo provides automated reporting to the EC for open data stored within it, so evidence of the commitment from Fed4FIRE+ and experimenters to provide open experiment data can be easily verified.

8.3 Funding Available

Funding to cover the experimenter's costs in preparing the ORD data package is available from the Fed4FIRE+ Federator. This is additional to the support funding for experiments, and will be paid to a experimenter upon confirmation that their experiment data package is complete and uploaded into the Fed4FIRE+ approved data repository, Zenodo.

The funding available is capped to an upper limit of €500.

8.4 Process

The process for ORD in Fed4FIRE+ is shown in Figure 1. The left-hand column shows activities by the experimenter, and the right hand column shows activities by the Federator.

At experiment proposal time, the experimenter decides whether they want to open data. If they want to keep data confidential, they need to provide satisfactory reasons why not in their proposal. Valid reasons will not prejudice against funding for experiment proposals. If experimenters want to open data, they must complete a basic data management plan and include this with the proposal submission. If the proposal (including the basic DMP) is accepted, in addition to providing the experiment funding, the Federator puts aside funding to cover the experimenter's extra costs in preparing the ORD package.

After the experiment is complete, the experimenter has another opportunity to decide whether they want to open their research data. If they wish to keep their data closed, they need to provide reasons in their experiment report. If they wish to open data, they must complete a more detailed DMP, prepare a data package including metadata describing the experiment data and upload the data package to Fed4FIRE+'s approved data repository, Zenodo. Zenodo will issue a Digital Object Identifier, and this must be submitted to the Federator. The Federator will check the existence and completeness of the data package, and if all is well, will authorise a cost claim for the experimenter covering their costs for opening data (up to a limit of €500).

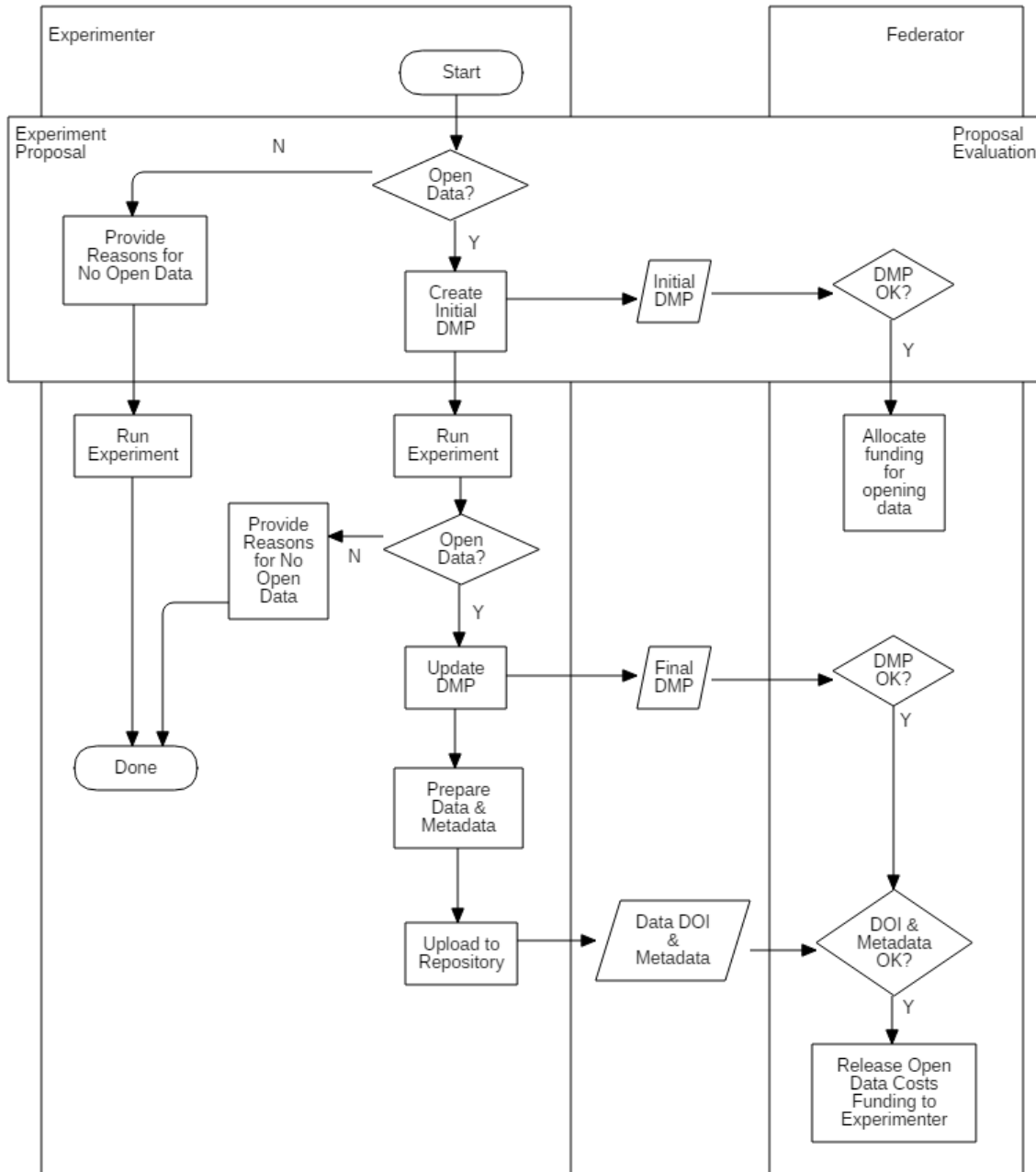


Figure 1: Fed4FIRE+ Open Research Data Process

9 Proposal template

The use of a specific proposal format as described in this section is mandatory. The template (can be found as download on the Fed4FIRE+ website together with this Call information) is limited in size and is focusing on “what experimenters want to do” and “what the expected result is”.

- Section A** Information page and Summary (300 word summary)
The information in this section may be used in public documents and reports by the Fed4FIRE+ consortium.
- Section B** Description and Expected Results (target length 6 pages)
describing the details on the planned experiment (what do you hope to obtain, how, why is it relevant,...). This section should also include all information with respect to the State-of-the-Art to show the innovative character of the experiment and the expected business impact
- Section C** Requested Fed4FIRE+ tools, testbeds and facilities (1 page, standard form)
The information in this section needs to be collected in collaboration with the Fed4FIRE partner acting as patron on this experiment. For this section a specific format needs to be used, which is attached to this document and available for download.
- Section D** Compliance check (max. 1 page, standard form to be provided by the Fed4FIRE+ Patron)
This section contains the formal statement of the Fed4FIRE+ partner(s) acting as patron on this experiment that he/she has been informed about your proposed experiment and that he agrees that it can be carried out on the required testbed(s). To be able to complete this form, the Patron needs to be informed about the proposal itself. Therefore, a “feasibility-check” deadline is set, by which the Patron needs to have received the draft proposal to be able to complete this form.
- Section E** Background and qualifications (target length 1-2 pages)
This section describes the proposing experimenters and includes an overview of the activities, your qualifications, technical expertise and other information to allow the reviewers to judge your ability to carry out the experiment.
- Section F** Expected feedback to the Fed4FIRE+ Consortium (target length 1-2 pages)
This section contains valuable information for the Fed4FIRE consortium and should indicate the expected feedback the Fed4FIRE consortium can expect from the use of its federated facilities after carrying out your experiment. This information is essential in view of the sustainability of the facilities and use of tools and procedures. Note that the production of this feedback is one of the key motivations for the existence of the Fed4FIRE open calls.
- Section G** Requested funding (1 page, standard form).
This section provides an overview of the budgeted costs and the requested funding. A split is made in personnel costs, other direct costs (travel, consumables,..) and indirect costs (see section 6). This section also includes the split between the budget allocated to the experimenter and the budget allocated to the Patron(s), clearly arguing this split (max. €5 000 in total for the patron(s)). It is thus possible to have e.g. one patron providing specific testbed resources and setup for €3 500 and another patron offering consulting help for €1 500 for the same experiment.
- Section H** Participation in previous Open Calls of the Fed4FIRE+ project.
This section provides information on previous participation in Open Calls of the Fed4FIRE+ project:

- Parties who have submitted proposals in previous calls which were NOT selected for funding should indicate the exact dates and details of the previous submissions.
- Parties who have submitted proposals in previous calls which were selected for funding should indicate the difference between the current proposal and the previously submitted proposal.
- Parties belonging to a legal entity of which other groups have submitted proposals in previous calls also need to indicate the difference between the current proposal and the previously submitted proposals.

Section I Survey.

This survey contains a list of specific requirements which you expect your experiment has for our federated testbeds. This survey will be done through a specific template which will become available on-line. This survey is an integral part of your proposal. Proposing parties who do not complete this survey by the set deadline are not eligible for evaluation.

The survey responses will remain within the Fed4FIRE consortium and will be used for reports and evaluation of the Fed4FIRE tools, testbeds and concept. The results will not be forwarded to the reviewers and will consequently not influence the scoring of your proposal during the evaluation process.

Section J Data Management

This section begins with the question: “Will you provide a complete, publicly-accessible dataset of your experiment results and supporting data, uploaded in Fed4FIRE+’s chosen repository?”

For the Answer “NO”: The experimenter needs to provide reasons why they will not make their experiment data open as part of the proposal. Guidance on opt out reasons can be found in Section 8.1.

For the Answer “YES”: The experimenter needs to fill in the table provided in the template, and this becomes the initial Data Management Plan, to be submitted with the experiment proposal. Guidance notes are provided in the table.

10 Support during experiment and the role of the Patron

Experimenters in this open call category have access to basic and advanced support:

A. Basic support

- Guaranteeing that the facility is up and running (e.g. answering/solving "could it be that server X is down?")
- Providing pointers to documentation on how the facility can be used (e.g. "how to use the virtual wall testbed" => answer: check out our tutorial online at page x")
- Providing pointers to technical questions as far as relevant (e.g. answering "do you know how I could change the WiFi channel" => answer: yes, it is described on following page: y"; irrelevant questions are for example "how to copy a directory under Linux")
- This support will be handled through the support forum detailed at <http://doc.fed4fire.eu/support.html>

B. Dedicated (advanced) support includes all of the following supporting activities by the patron:

- Deeper study of the problem of the experimenter: invest effort to fully understand what their goals are, suggest (alternative) ways to reach their goals. To put it more concretely (again using the example of the Virtual Wall testbed), these experimenters do not need to know the details on the Virtual Wall or how it should be used, they will be told what is relevant to them and can focus on their problem, not on how to solve it.
- Help with setting up the experiments (e.g. "how to use the virtual wall" => answer: the tutorial is there, but let me show you how what is relevant for you, let me sit together with you while going through this example and let us then also make (together) an experiment description that matches what you are trying to do.
- (Joint) solving of practical technical problems (e.g. "do you know how I could change the WiFi channel" => yes, it is described on page y, in your case you could implement this as following: ..., perhaps we should quickly make a script that helps you to do it more easily, ...)
- Custom modifications if needed: e.g. adding third-party hardware and preparing an API for this.
- Technical consultancy during/after the experiments (e.g. "I do get result x but would have expected y, what could be the problem?")

It is essential that you get in contact with the Fed4FIRE+ partner in charge of the testbed(s) you will use for your experiment to discuss your experiment and the specific requirements. Each proposing party must therefore contact the Fed4FIRE+ consortium regarding its submission to identify a possible Patron. The proposing party must submit its draft proposal to this Patron. The feedback by the Patron is provided in section D of the proposal.

The role and support by the Patron will be reflected in the budget (see section G of the proposal). At least one Patron is needed per experiment, but more are possible.

11 Budget & Payment scheme

As the experimenter will be linked to the Fed4FIRE+ consortium as 3rd Party receiving financial support, specific arrangements exist with respect to financial costs and payment schemes:

11.1 Compliance rules

- As a 3rd Party, the proposing party needs to include an overview of the estimated costs in its proposal at the time of submission. Costs consist of personnel costs, direct costs (such as travel, consumables, etc.) and indirect costs. The costs of a 3rd Party have to comply with the rules and the principles mentioned in Section I, Article 6 (Eligible and ineligible costs) of the H2020 AGA — Annotated Model Grant Agreement (see http://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/amga/h2020-amga_en.pdf), in the same way as the beneficiaries, and must be recorded in the accounts of the 3rd Party. In other words, the rules relating to eligibility of costs, identification of direct and indirect costs and upper funding limits apply. Equally those concerning controls and audits of Section I, Article 22 of the H2020 AGA.

11.2 Budget

- The maximum requested funding for each experiment in this Call is set at:
 - 60k euro for Medium Experiments and
 - 100 k euro for Large Experiments
- The budget covers the costs for:
 - the experimenter including the costs for:
 - getting acquainted with the testbed
 - executing the experiment
 - reporting feedback about the federation framework
 - submitting the required documents
 - attending the required meetings (travel)
 - the Fed4FIRE+ partner(s) acting as Patron(s) including the costs for:
 - supporting the proposer during the preparation and execution of the experiment
 - specific adaptation of the testbed to run the experiment
 - providing feedback and quality-check on the submitted reports and materials by the experimenter.
- The budget can be split in a flexible way between the experimenter and the Patron but the split needs to be provided and argued in the proposal (with a max. total of €5000 for the patron(s)).

11.3 Submission of invoices

- The proposer will need, if its experiment is selected for funding:
- To submit an invoice for 75% of the budget allocated to the 3rd Party which will be paid by imec as coordinator upon an approval of the report by the Fed4FIRE+ consortium.
- To submit an invoice for 25% of the budget allocated to the 3rd Party which will be paid by imec as coordinator upon receiving a positive evaluation report by the EU appointed reviewers following a formal review by the EU representatives.
- Payments to the Fed4FIRE+ partner acting as Patron will be made internally within the consortium.

12 Access to Foreground information from the project

As indicated by the EC Guidelines, a 3rd Party is paid in full for its contribution made to a project by the coordinator. As a consequence 3rd Parties do not have any IPR rights on the foreground of the project.

13 Reporting

As the experimenter will be linked to the Fed4FIRE+ consortium as 3rd Party receiving financial support, no input will be required for any of the regular project reports which the Fed4FIRE+ consortium needs to submit to the EU.

A final report needs to be submitted after conclusion of the experiment. A specific template needs to be used (can be found as download on the Fed4FIRE+ website together with this Call information) and will include:

- Part A. Summary
- Part B. Detailed description
This section describes the details on the experiment and provides information as you have been collecting this from your point of view and from your business. It includes:
 - B.1 Concept, Objectives, Set-up and Background
 - B.2 Technical Results & Lessons learned
 - B.3 Business impact
- Part C. Open Research Data
This section provides feedback on the actions taken by the proposer in the framework of the Open Research Data initiative. If you have opted out of this initiative, please provide the reasons. If you have opted in, please provide the Final Data Management Plan and all necessary information to show that a complete, publicly-accessible dataset of your experiment results and supporting data, has been uploaded in Fed4FIRE+'s chosen repository.
- Part D. Feedback to Fed4FIRE+
This section contains valuable information for the Fed4FIRE consortium and describes your experiences by running your experiment on the available testbeds. Note that the production of this feedback is one of the key motivations for the existence of the Fed4FIRE+ open calls. It includes:
 - C.1 Resources & tools used
 - C.2 Feedback based on design/set-up/running your experiment on Fed4FIRE+
 - C.3 Why Fed4FIRE+ was useful to you

This report will not only serve as an evaluation tool to judge payment of the experimenter, but will mainly serve as input to the Fed4FIRE sustainability plans, evaluation of the user-friendliness of the Fed4FIRE tools and identification of missing gaps in both testbeds and tools.

Part of this report may be used by the Fed4FIRE+ consortium for inclusion in their reporting documents to the EU and in public presentations. Inclusion of confidential information should therefore be indicated and discussed with the Fed4FIRE+ consortium.

This report will also be used for the formal review by the European Commission.

14 Criteria for evaluation and ranking of experiments

Proposals can only be submitted by eligible parties (cfr section 3):

Evaluation and ranking will be carried out by an external review panel. Selection will mainly be based upon:

- Criteria I. A degree of industrial and/or scientific innovation including a motivation for the experiment. (**Error! Reference source not found.** of the Proposal Template)
The score given here should reflect the degree of innovation: if an experiment is pushing the boundaries of its domain, then it should get a higher score here than experiments testing trivial things. In order to demonstrate these criteria, the proposer may opt to indicate the State of the Art in the appropriate field.
- Criteria II. A degree of industrial and/or scientific relevance (**Error! Reference source not found.** of the Proposal Template)
This score should reflect the industrial relevance including the expected and projected impact on the experimenter through product development or the scientific relevance and the projected impact on the organisation
- Criteria III. Clarity and methodology (**Error! Reference source not found.** of the Proposal Template)
The experiment should be scientifically and/or technically sound. There should be a clear problem statement, a solid experiment design, a good methodology, etc.
- Criteria IV. An appropriate scale and complexity of experiment in respect to its implementation and execution in the scope of Fed4FIRE+ and defined time frame (**Error! Reference source not found.** of the Proposal Template)
Use of only a single testbed is acceptable, but multi-testbed experiments are preferred. No distinction is made between achieving this by running the same experiment in sequence on multiple testbeds (e.g. to evaluate different wireless environments), or by running a single experiment that relies on resources from different testbed at the same time. If however proposals have made their design artificially more complex than needed just in order to use multiple testbeds, then the score will be lower. Similarly, if proposals have made their designs too trivial while you can easily identify opportunities for involving other testbeds that would have made the experiment stronger, then the score will also be lower. In order to optimise the design of the experiment, the proposer should seek information on the available testbeds.
- Criteria V. Relevance for Fed4FIRE+ framework in terms of planned facility and tools utilization and potential feedback to the project on their usage (**Error! Reference source not found.** of the Proposal Template)
The Fed4FIRE consortium is seeking feedback regarding the available tools, procedures and testbeds. Proposals which can indicate that more information and feedback on the use of these tools and procedures will be provided will get a higher score. So the more of the Fed4FIRE tools and APIs that an experiment will use, the better. If they need to use additional non-Fed4FIRE tools, that is

not a problem as long as they clearly indicate the added value of these additional tools.

Criteria VI. Indication on possible future follow-up experiments and how this can support the sustainability of the federated testbed facilities. (**Error! Reference source not found.** of the Proposal Template).

The proposer may indicate possible follow-up projects and experiments which can contribute to the sustainability of the Fed4FIRE facilities. The quality, the size and the expected feasibility to carry out these future experiments will be reflected by the score in this criterion.

Criteria VII. The proposer should exhibit technological expertise and quality. This information must be included in **Error! Reference source not found.** of the Proposal Template.

Criteria VIII. Preference is given to proposals originating from new players in the field. Therefore the following restrictions will be implemented:

- parties who have submitted a proposal in previous calls of Fed4FIRE+ and which were selected for funding are allowed to submit a new proposal only when clear distinction can be made with previous submitted proposals.
- Parties who have not submitted or been participating in previous calls of the Fed4FIRE+ project but are belonging to same legal entity as proposers which have submitted proposals in previous calls, are eligible in case they can clearly identify the difference with previous submitted proposals by the other groups.
- This information must be included in H of the Proposal Template.

Amongst all above listed criteria, Criteria I, II and V will be weighted higher.

The proposed experiment must be executed on the available Fed4FIRE+ testbeds. This competitive call allows for both experiments using multiple testbeds (in parallel and/or in sequence) and experiments using a single testbed. Information about the [current Fed4FIRE+ testbeds is available at the dedicated pages](#)¹. The proposed experiment must use the experimentation tools provided by Fed4FIRE+ in order to provide feedback to the project about their usefulness and maturity in a final report. In justified cases additional external tools may be used.

5.2 EXPERIMENT PROPOSAL TEMPLATE



Green highlighted areas to be filled

6th Fed4FIRE+ Open Call - Experiments “Medium”

with focus on “Wireless Experimentation”

Full title of the existing project you wish to join:	Fed4FIRE+: Federation for FIRE
Acronym of the existing project:	Fed4FIRE+
Grant agreement number of existing project:	732638
Type of instrument:	Research and Innovation Action

Full title of your project
Acronym of your proposal (optional)

Date of preparation of your proposal: **xx/yy/201x**

Version number (*optional*):

Your organisation name: **Your organisation name**

Your organisation address: **Your organisation address**

Name of the coordinating person: **Name of the coordinating person**

Coordinator telephone number: **Coordinator telephone number**

Coordinator email: **Coordinator email**

(this will be the email address to which the Acknowledgement of Receipt will be sent)

Provide here the title of your proposal

Section A Project Summary

(Maximum 300 words – summary of your proposed work)

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum. Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum. Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum. Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum. Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Remark: The information in this section may be used in public documents and reports by the Fed4FIRE+ consortium.

Section B Detailed Description and Expected Results (target length 6 pages)

This section describes the details on the planned experiment (what do you hope to obtain, how, why is it relevant). This section should also include all information with respect to the State-of-the-Art to show the innovative character of the experiment and the expected business impact. Suggested sections include:

B.1 Concept and objectives

Describe in detail the objectives of your proposed experiment. These objectives should be those achievable within your proposed action, not through subsequent development. Preferably they should be stated in a measurable and verifiable form.

B.2 Business impact

Describe how this experiment may impact your business and product development by indicating the way how this experiment fits in your activities.

Having close contacts with possible end-users during this experimental phase might be used to illustrate the business impact of your experiment.

B.3 Description of State-of-the-Art

Describe in detail how this experiment compares to the State-of-the-Art in the field covered by the experiment. Are there similar experiments, products, services,.. on the market? Is this experiment incremental to existing work?

B.4 Methodology and associated work plan

Provide a workplan which eventually can be broken down into work packages¹ (WPs). Provide clear goals and verifiable results and also a clear timing.

¹ A work package is a major sub-division of the proposed work with a verifiable end-point - normally a deliverable or a milestone in the overall action.

Section C Requested Fed4FIRE+ tools, testbeds and facilities (target length 1 page)

Please check the Fed4FIRE+ testbed or multiple testbeds which will be required for your experiment

Please use www.fedfire.eu to get details on the specific testbeds or contact@fed4fire.eu.

Wired networking testbeds		
	Virtual Wall (imec)	
	PlanetLab Europe (UPMC)	
	PL-LAB (PSNC)	
	Geant Testbed as a Service (GTS) (Nordunet)	

Wireless/5G/IoT testbeds		
	w-iLab.t (imec)	
	Portable wireless testbed (imec)	
	CityLab (imec)	
	NITOS (UTH)	
	Netmode (NTUA)	
	SmartSantander (UC)	
	FuSeCo (FOKUS)	
	PerformLTE (UMA)	
	IRIS (TCD)	
	LOG-a-TEC (JSI)	
	R2lab (Inria)	

OpenFlow testbeds		
	i2CAT OFELIA island	
	NITOS (UTH)	
	Virtual Wall (imec)	

Cloud computing testbed		
	Virtual Wall (including GPUlab) (imec)	
	Exogeni (UvA)	
	Grid5000 (Inria)	

Other		
	Tengu – big data (imec)	

Please provide here more information on why specific testbeds will be required for your experiment (max. ½ page)

Provide here the title of your proposal

Section D Compliance check (max. 1 page)

Each proposing party must contact the Fed4FIRE+ consortium regarding its submission to identify a possible Patron. This Patron will in most cases be the Fed4FIRE+ partner responsible for the Testbed the proposing experimenter will use during its experiment. The proposing party must submit its draft proposal to this Patron by the set deadline for the Feasibility Check. The Patron completes the form below and this signed form is copied by the proposer into this section of the proposal.

It is advised you get as soon as possible in contact with the Fed4FIRE++ in charge of the testbeds you intend to use and discuss with him/her your proposal.

I, (name),

representing (Fed4FIRE+ Partner)

hereby confirms to have been informed about the

proposal (proposal name)

being prepared by (experimenter organisation)

and to be submitted to the Fed4FIRE+ Open Call -5.

I, acting as Patron for the above mentioned experiment, hereby confirms that the proposed experiment can be carried out on the testbeds as indicated in Section C of this proposal.

Signature

Provide here the title of your proposal

Section E Background and qualifications (target length 1-2 pages)

This section describes the proposing SME and includes an overview of the activities, your qualifications, technical expertise and other information to allow the reviewers to judge your ability to carry out the experiment.

Section F Expected feedback to the Fed4FIRE+ Consortium (target length 1-2 pages)

This section contains valuable information for the Fed4FIRE+ consortium and should indicate the expected feedback the Fed4FIRE+ consortium can expect from the use of its federated facilities after carrying out your experiment. This information is essential in view of the sustainability of the facilities and use of tools and procedures. Note that the production of this feedback is one of the key motivations for the existence of the Fed4FIRE+ open calls.

Section G Future plans (target length 1 page)

This section contains information regarding expected possible follow-up experiments, new initiatives, new projects which may follow out of the experiment as proposed in this Open Call.

The proposer may indicate possible follow-up projects and experiments which can contribute to the sustainability of the Fed4FIRE+ facilities. The quality, the size and the expected feasibility to carry out these future experiments will be reflected by the score in this criterion.

These future plans can be new experiment with Fed4FIRE+, a new research project, internal projects, product commercialization.... As the objective of Fed4FIRE+ is to provide an incentive, seed budget or initial assistance in your business or research, any new initiative triggered by this experiment is acceptable to be listed. The future plans do not have to exclusively impact the future of Fed4FIRE+.

Section H Requested funding (form to be completed)

This section provides an overview of the budgeted costs and the requested funding. A split is made in personnel costs, other direct costs (travel, consumables,..) and indirect costs. This section also includes the split between the budget allocated to the experimenter and the budget allocated to the Patron(s), clearly arguing this split (max. €5 000 in total for the Patron(s)). It is thus possible to have e.g. one patron providing specific testbed resources and setup for €3 500 and another patron offering consulting help for €1 500 for the same experiment.

For the travel budget, see the needed travels in the call document.

Besides the table below, extra information can be provided to support the requested funding and which may help to judge the cost to the Fed4FIRE+ project.

Please show your figures in euros (not thousands of euros)

H.1 Budget Experimenter:

	Total PM	Cost
1. Personnel costs (incl. indirect costs)		
2. Other costs (incl. indirect costs)		
3. Total costs (Sum of row 1 and 2)		

H.2 Budget Patron:

	Total PM	Cost
1. Personnel costs (incl. 25% indirect costs)		
2. Other costs (incl. 25%. Indirect costs)		
3. Total costs (Sum of row 1 and 2)		

In row 1, insert your personnel costs for the work involved.

In row 2, insert any other costs, for example equipment or travel costs.

For the Experimenter all numbers must include indirect costs, for the Patron, indirect costs follow the H2020 guidelines and are defined as 25%.

Provide here the title of your proposal

Section I Participation in previous Open Calls of the Fed4FIRE+ project. (1-2 pages)

Parties who have submitted proposals in the previous Open Calls of the Fed4FIRE+ project are allowed to re-submit.

Information only to be provided if one of the following conditions apply:

- Parties who have submitted proposals in previous calls which were NOT selected for funding should indicate the exact dates and details of the previous submissions.
- Parties who have submitted proposals in previous calls which were selected for funding should indicate the difference between the current proposal and the previously submitted proposal.
- Parties belonging to a legal entity of which other groups have submitted proposals in previous calls also need to indicate the difference between the current proposal and the previously submitted proposals.

Section J Open Research Data

Will you provide a complete, publicly-accessible dataset of your experiment results and supporting data, uploaded in Fed4FIRE+'s chosen repository?	YES or NO
For the Answer "NO":	The experimenter needs to provide reasons why they will not make their experiment data open as part of the proposal. Guidance on opt out reasons can be found in Section 8.1.
For the Answer "YES":	The experimenter needs to fill in the following table, and this becomes the Initial Data Management Plan, to be submitted with the experiment proposal. Guidance notes are provided in the table.

Initial Data Management Plan (DMP)

Section	DMP Category and Question	Initial DMP	Fed4FIRE+ Guidance Notes
			Y = mandatory to answer question, O = optional to answer, N/A = not applicable
0	Experiment Information		
	Name of Experiment	Y	
	Names of Experimenters	Y	
	Experimenters' Organisations	Y	
	Fed4FIRE+ Call ID	Y	
	Experiment Start Date	Y	
	Experiment End Date	Y	
	Fed4FIRE+ Testbeds	Y	
	Fed4FIRE+ Sponsor	Y	
1	Data Summary		
	What is the purpose of the data collection/generation and its relation to the objectives of the project?	Y	This should be the abstract of experiment from proposal including objectives of collecting the experiment data.
	What types and formats of data will the project generate/collect?	Y	Initially this can be an estimate. In the final DMP this should be a statement of the formats, so it can go into the metadata.
	Will you re-use any existing data and how?	O	If any external data is anticipated before the experiment starts, state it here. If any external data has been used during an experiment, it must be stated, along with any license terms or stipulations.

Section	DMP Category and Question	Initial DMP	Fed4FIRE+ Guidance Notes
			Y = mandatory to answer question, O = optional to answer, N/A = not applicable
	What is the origin of the data?	Y	This is the expected source of the data before the experiment runs, and the actual source of data once the experiment is complete.
	What is the expected size of the data?	O	Initially this can be an estimate. In the final DMP this should be the actual size of the data.
2	FAIR² data		
2.1	<i>Making data findable, including provisions for metadata</i>		
	Are the data produced and/or used in the project discoverable with metadata, identifiable and locatable by means of a standard identification mechanism (e.g. persistent and unique identifiers such as Digital Object Identifiers)?	Y	Initially, this should be a statement committing that the experiment data will be discoverable. When the experiment is complete, the experiment data's Digital Object Identifier (DOI) and metadata should be cited. Fed4FIRE+'s repository of choice, Zenodo, allocates a DOI at upload time, and allows keywords to be entered into a form. These keywords will form part of the metadata that allow the data to be discoverable.
	What naming conventions do you follow?	O	Initially this can be optional, although it is recommended to think of the naming conventions before the data is collected. After the experiment, this should cite the naming conventions used.
	Will search keywords be provided that optimize possibilities for re-use?	Y	This should always be YES - there will be or are keywords for search terms. The keywords should be stated here.
2.2	<i>Making data openly accessible</i>		
	What methods or software tools are needed to access the data?	O	If there are any special tools or methods needed to access the data (e.g. commercial software tools that can open the data's format), state them here.
	Is documentation about the software needed to access the data included?	O	If software tools are needed, cite the documentation.
	Is it possible to include the relevant software (e.g. in open source code)?	O	If possible, include or cite the software tools (e.g. sourceforge location)
2.3	<i>Making data interoperable</i>		

² FAIR is an acronym for “findable, accessible, interoperable and reusable”. See: Wilkinson, Mark D., Michel Dumontier, IJsbrand Jan Aalbersberg, Gabrielle Appleton, Myles Axton, Arie Baak, Niklas Blomberg et al. "The FAIR Guiding Principles for scientific data management and stewardship." *Scientific data* 3 (2016). <http://dx.doi.org/10.1038/sdata.2016.18>

Section	DMP Category and Question	Initial DMP	Fed4FIRE+ Guidance Notes
			Y = mandatory to answer question, O = optional to answer, N/A = not applicable
	Are the data produced in the project interoperable, that is allowing data exchange and re-use between researchers, institutions, organisations, countries, etc. (i.e. adhering to standards for formats, as much as possible compliant with available (open) software applications, and in particular facilitating re-combinations with different datasets from different origins)?	Y	The default position for Fed4FIRE+ is "yes - the data will be (or is) interoperable". This section should be a statement of commitment by the experimenter that the data will be (or is) interoperable.
	What data and metadata vocabularies, standards or methodologies will you follow to make your data interoperable?	O	Initially, this should be a statement of the formats intended for the data, together with citations of their definitions if applicable (e.g. RFCs etc.). For metadata, the experimenter should cite the anticipated metadata schemas by URL. After the experiment is complete, it should be a statement of the actual formats used, as well as citations to metadata schemas.
2.4	<i>Increase data re-use (through clarifying licences)</i>		
	How will the data be licensed to permit the widest re-use possible?	Y	Initially, this should be a statement of the intended license, which at least must permit open access. Once the experiment is complete, the data must be licensed under terms that permit open access, and the license must be named here. The default license is Creative Commons CC-BY 4.0, an open license that provides attribution of the creator.
	Are data quality assurance processes described?	O	If any QA procedures are observed, they should be stated - it is in the interest of the experimenter to describe these, as they will help the reusability of the data.
3	Allocation of resources		
	Who will be responsible for data management in your project?	Y	The person responsible for the data management should be named in both the initial and final DMP. This should be the principal experimenter.
4	Data security	N/A	Responsibility of Repository
5	Ethical aspects		

Section	DMP Category and Question	Initial DMP	Fed4FIRE+ Guidance Notes
			Y = mandatory to answer question, O = optional to answer, N/A = not applicable
	Are there any ethical or legal issues that can have an impact on data sharing? These can also be discussed in the context of the ethics review. If relevant, include references to ethics deliverables and ethics chapter in the Description of the Action (DoA).	Y	Legal, ethical and data protection issues must to be described in the initial DMP that forms part of the experimenter's proposal before the experiment runs, together with procedures for correct compliance with the applicable laws including the implications of storing the data for the long term in an open repository.
	Is informed consent for data sharing and long term preservation included in questionnaires dealing with personal data?	Y	The experimenter must specify methods for acquiring informed consent in their initial DMP.
6	Other issues		
	Do you make use of other national/funder/sectorial/de partmental procedures for data management? If yes, which ones?	O	If other DMP procedures are used, the experimenter should state them.

Section K Survey & Use of proposal information

Proposals are treated in a confidential way, meaning that only successful proposals may be disclosed to the Fed4FIRE+ consortium. Open calls previously organized by other FIRE projects were very successful and have revealed that many submitted non-granted proposals also contain very interesting and valuable information that could be used for setting up collaborations or to extract ideas for further improving the federated test infrastructures. Therefore, the project would like to have the opportunity to collect more detailed information and further use this information, also if the proposal is not selected for funding. In any case, the Fed4FIRE+ consortium will treat all information of this proposal confidentially. Three types of information usage are envisaged:

- Information which is part of the Sections A, C, D and F will be used within the Fed4FIRE+ project as input for tasks related to architectural optimizations, sustainability studies, etc. The same information can also be used in an anonymous way to create statistics and reports about this first open call. All proposals submitted to this competitive open call are obliged to allow this form of information access and usage.
- Other information belonging to this proposal might also be accessed by the Fed4FIRE+ consortium if allowed by the corresponding consortium. Any use of such information will be discussed and agreed upon with the proposers. Proposals have the freedom to select if they wish to support this kind of information usage.
- As part of the submission of your proposal, and in support of the Fed4FIRE+ project itself, a survey needs to be completed (Section I). This survey consists of a list of specific requirements which you expect your experiment has for our federated testbeds. Please be informed that the survey has been set up in general terms and some of the questions may not apply to your experiment. This survey and its responses are intended for internal use within the Fed4FIRE+ project and for the collection of information in view of the Fed4FIRE+ deliverables and reports. The survey and its responses will NOT be forwarded to the reviewing panel and will therefore have NO impact on the evaluation process. This survey is an integral part of your proposal and proposals submitted without completing the on-line survey will not be eligible.
The survey consists of a template available in Section I that needs to be completed.

The proposers are therefore asked to include the following statements below in their proposal and tick the corresponding boxes.

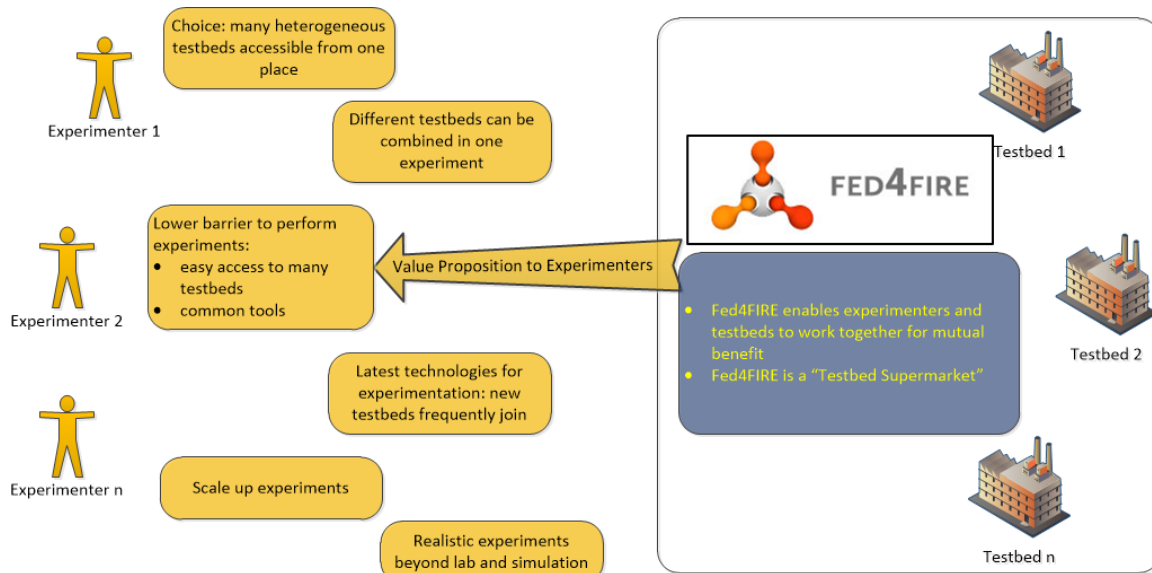
<p>I allow that the material provided in Sections A, C, D and F of this proposal may be accessed by the Fed4FIRE+ consortium, also if the proposal is not selected for funding. In any case, the Fed4FIRE+ consortium will treat all this information confidentially. It will be used within the Fed4FIRE+ project as input for tasks related to architectural optimizations, sustainability studies, etc. The same information can also be used in an anonymous way to create statistics and reports about this first open call.</p>	YES <input type="checkbox"/>	
<p>Furthermore, I allow that the other parts of this proposal may be accessed by the Fed4FIRE+ consortium, also if the proposal is not selected for funding. In any case, the Fed4FIRE+ consortium will treat all information of this proposal confidentially. Any use of this information will be discussed and agreed upon with the proposers.</p>	YES <input type="checkbox"/>	NO <input type="checkbox"/>

Section L Questions to experimenters

Part A – Sustainability

Fed4FIRE+ wants to become a sustainable federation. We are identifying the key factors for our success and we hope for your collaboration in helping us prioritise our next moves so that we can serve you better. The questionnaire included in this section is therefore designed in such a way that it can help us understand which aspects are more valuable to you.

The next picture shows some ideas of how we may bring a valuable service to you. Please take a moment to go through it before completing the following survey.



In the survey table below, we would like to assess which aspects of the federation are perceived as most valuable by our experimenters. The Value column should be filled in as follows:

X = no opinion or not applicable to your experiment/ environment
1=not valuable 2=nice side-effect 3=important value 4=Very important value

<i>Thanks to Fed4FIRE+, I ...</i>	Value (X or 1..4)	Comments
... have access to a large and ideal set of different technologies (sensors, computing, network, etc.), provided by a large amount of testbeds. This way I can experiment with edge technology in all current research trends.		
... have access to resources that otherwise would not be affordable.		
... have access to testbeds that are geographically distributed.		
... the user experience is that I only have to deal with a single service provider (i.e. single point of contact and service) instead of dealing with each testbed on my own. This relates to many aspects of experimentation such as authentication, learning about available resources, reserving those resources, controlling them during the experiment, getting the results out of your experiment, hiring training services, getting support, etc.		
... can experiment using a small set of common well-documented experimenter tools. This brings me several benefits: simplicity (since those tools can hide many of the testbeds' complexities), a single federated interface, a uniform input/output from different systems, and allows me to use a single user account while experimenting with resources over all these different testbeds. All these benefits result in a lower entry barrier, allowing me to experiment quickly, without investing much effort in learning how to work with a plethora of different tools for the different testbeds.		
... can reduce the effort required to experiment and hence to take my product to the market (since the federation provides me easy access to the resources at the different testbeds, and user-friendly experimenter tools as described above).		

<i>Thanks to Fed4FIRE+, I ...</i>	Value (X or 1..4)	Comments
... have access to a wider experimenters community. This leads to a greater impact of results, shared dissemination and the possibility to share experience and knowledge with other experimenters.		
... acquire new competences to, e.g., optimize my solutions. This way I can increase my own technical scope and competitiveness.		
... have a trustworthy environment for my experiments: my data is protected and the privacy of me and my experiment is guaranteed.		
... can experiment in a controlled environment where experiments are repeatable. This allows the thorough execution of performance assessments and allows easy comparison of results.		
... feel that I pick what I need beyond my initial ideas because of the greater choice in facilities and resources, which leads to greater inspiration (supermarket effect).		
... can experiment in a unique environment for experimentation that goes beyond the lab environment and enables real world implementation.		
... have the support I need to successfully complete my experiment: the federation provides a federation-wide First Level Support Service (hotline), and I can get in touch with the experts of every testbed using the same mechanism.		
... have service level guarantees concerning the facilities used in my experiment (availability during my experiment, incident solving time,...)		

The above table concerns characteristics of the federation that we already identified as potentially being of value to our experimenters. In those cases it is sufficient to gather feedback about how valuable they are in reality for our experimenters. However, regarding some other aspects there is more indistinctness within the project. Therefore the second part of this sustainability section of this experimenter survey adopts the format of open questions. **Hence we would like to ask you to answer the following questions.**

1. Why do you want to join the open call? Is this mainly to receive funding for doing your research about a specific topic that is on your roadmap today? Is this because you want to get some experience with Fed4FIRE+ resources to be able to use them again in the future for other topics? Do you have other reasons?

<Please type your answer here>

2. Would you propose an experiment without the funded open call? In other words, would you also be interested in experimenting on Fed4FIRE+ in an unfunded open access scheme? Why (not)?

<Please type your answer here>

3. The federation provides several measures to lower the barrier for an experimenter as much as possible: you can experiment with all the offered resources using the same small set of common tools, detailed documentation is provided, you only need a single user account to experiment on all testbeds, there is a First Level Support service, etc. **Which of these things should the federation at least offer to allow experimentation without funding?** Are there any other items that the federation should provide to make it feasible to experiment on our facilities without receiving any funding for doing so?

<Please type your answer here>

4. Currently we support the experimenters with a First Level Support service (hotline) operated by the same people that operate the NOC of the Géant network. Next to that we provide an active community forum where experimenters can easily get in contact with experts of all the Fed4FIRE+ testbeds for advanced online support. **Are there any other kinds of support that you would expect from the federation, which is not available today?** For instance, should the federation provide some kind of consultancy service that can guide you through every step of the process of transforming your idea into an actual successful experiment? Would you be willing to pay for that consultancy service (e.g. instead of paying for the usage of the resources). Can you think of any other additional support that we could offer?

<Please type your answer here>

Part B – Requirements

The goal of this part of the survey is to get a feeling of the requirements that your experiment imposes on the Fed4FIRE+ federation of testbeds. For the listed requirements we are mainly trying to prioritize requirements that are already on our radar, based on what our potential experimenters really need. Next to those requirements, we are very keen to receive any new requirement that you can think of that also needs to be fulfilled when supporting your experiment. For this we have created the possibility to add as many new requirements as you see fit.

The questions of this part of the survey are presented in different tables, clustered around the different steps that an experimenter has to go through when running an actual experiment. In every of those tables, the Priority column should be filled in as follows:

X = no opinion or not applicable to your experiment/ environment
1=not required 2=nice to have 3=important 4=must have

L.1 Requirements related to resource discovery

The requirements listed in this table are all related to the very first thing that an experimenter does: learning about the different testbeds, and about which specific resources that they can offer.

	When discovering the different resources that Fed4FIRE+ can offer me for my experiment, I require ...	Priority (X or 1-4):	Comments and further details
1-1	That I can browse some kind of resource catalogue to look for appropriate resources on a high level. Such a catalogue is limited to information such as: testbed X is a testbed for WiFi experiments in an office environment, testbed Y is a testbed for testing cloud applications, etc.		
1-2	That Fed4FIRE+ provides a detailed view on what node capabilities are available on every testbed of the federation (e.g. mentioning information for every resource of a testbed regarding CPU speed, RAM, supported 802.11 technology, optical networking interfaces, etc).		
1-3	That the above view on node capabilities is the same across the different testbeds of the federation. This means that when describing the characteristics of resources, all testbeds should adopt the same units (e.g. represent RAM always in MB, and not sometimes in MB and sometimes in GB) and use the same parameter names for aspects that mean the same (e.g. always talk about “RAM”, and not “RAM” on some testbeds, “working memory” on some others and just “memory” on a third group of testbeds).		
1-4	That next to browsing through information about what is		

	available, that I can actively search for the existence of resources with certain characteristics by defining a specific query (e.g. something that is similar to an SQL query, e.g. select resources from all testbeds where RAM >= 8 GB)		
1-5	That I know the location of the site where resources are located. Per site, this location information can be exactly the same for all resources.		
1-6	That for nodes that have static network connections to other nodes in the same testbed, that it should be possible to identify the corresponding physical topology. In the wired domain this means that you can know how the nodes are connected to each other. For wireless resources this means that you know which resources are in transmission range of each other.		
1-7	That I have accurate location information about the actual resources that I will use (1 m accuracy), typically important for wireless nodes.		
1-8	For virtual resources, that I know their physical host and the actual location.		
1-9	That I can assess which testbeds/resources are more reliable than others (both in terms of provided hardware, software, and wireless interference, possibly based on historical health information about the resources and their environment)		
1-10	<i>If you have any additional requirements regarding resource discovery, please insert them here. Create as many new rows in this table as needed.</i>		
1-11			
1-12			
1-13			

L.2 Requirements related to resource selection and reservation

Once an experimenter has learned which resources are available at every testbed, he/she can then design its experiment appropriately. When setting up the corresponding experiment, the first thing that needs to be done is selecting resources to be included in the experiment, and reserving them for the experiment for a certain moment in time.

	When selecting and reserving resources that I want to include in my Fed4FIRE+ experiment, I require ...	Priority (X or 1-4):	Comments and further details
2-1	That when browsing through the resource descriptions, that I can manually select every node that should be added to my experiment. Think of an experience similar to online shopping and putting resources in your shopping cart.		
2-2	That I can select suitable resources for inclusion in my experiment by defining a specific query (e.g. something that is similar to an SQL query, e.g. select all resources from Virtual Wall where nr_ethernet_cards >= 6)		
2-3	That I can temporarily install my own equipment at a Fed4FIRE+ testbed for testing, and select it to be included in my experiment.		
2-4	That the mechanism for registering my own equipment at a testbed is standardized, allowing me to register that equipment at different testbeds in exactly the same manner.		
2-5	That I can reserve resources. It is OK for me that they are shared with others (soft reservation, e.g. requesting a virtual machine that will be deployed on a physical server that is used by other experiments also), as long as I know that I will also have guaranteed access to them.		
2-6	That I can reserve resources. They have to be exclusively assigned to me (hard reservation, e.g. reserving a virtual machine that will be deployed on a physical machine that is dedicated to your experiment only)		
2-7	That next to adding resources to my experiment right now (instant reservation), that I can also define a reservation for any moment in the future (future reservation, e.g. tomorrow from 9AM-5PM).		
2-8	That situations are avoided where a have to wait days or weeks before being able to use the testbed because of long reservations of others.		

2-9	That I can reserve nodes exclusively for myself for a longer period (days or weeks)		
2-10	That a reservation is approved or rejected quickly (within a few minutes).		
2-11	That I can easily reserve resources across multiple testbeds using the same common tools. These should also be as user-friendly as possible, abstracting the complexity of the underlying infrastructures for me as much as possible. This way I can focus on the experiment design itself instead of learning how to work with numerous testbed-specific tools.		
2-12	That when reserving resources across multiple testbeds, that there is guidance in finding the first appropriate time when all the resources that I want across the testbeds would all be available.		
2-13	That I can use a single Fed4FIRE+ account to select and reserve resources at all different testbeds of the federation. So even when using one common tool for reservation at the different testbeds, I don't want to remember a different username/password combination for every testbeds, and I also don't want to register again at every testbed that I want to use. Of course, registering for that one Fed4FIRE+ account should also be straightforward.		
2-14	That if testbeds decide to assign me a certain reservation quota (e.g. based on my profile such as student, post-doc, professor, paying customer, etc), that I can request a temporary increase of my quota if really need it (e.g. before a paper deadline)		
2-15	That the testbeds and/or the federation guarantee a certain Service Level to me regarding the execution of my experiment (availability of resources, reliability of resources (uptime/downtime), responsiveness of support services, privacy guarantees, etc).		
2-16	That I can dynamically scale my resources up and down according that what my experiment needs during its execution. For instance if a server deployed on a VM gets overloaded, I should be able to assign more resource (RAM, CPU cores, etc.) to that running VM, and/or should be able to add a second VM to my running experiment on which I deploy a second instance of that server.		

2-17	That if I reserved a number of resources at a testbed, that I can divide them over different independent experiments that I am doing at the same time. It should be possible to easily address/group the resources from one experiment.		
2-18	<i>If you have any additional requirements regarding resource selection and reservation, please insert them here. Create as many new rows in this table as needed.</i>		
2-19			
2-20			
2-21			
2-22			

L.3 Requirements related to using the resources (deployment and basic usage)

Once an experimenter has added the resources to the experiment, the next step is the deployment of those resources for that experiment, and basic usage of the resources. This section tries to capture the corresponding requirements.

	When using the resources that I included in my Fed4FIRE+ experiment, I require ...	Priority (X or 1-4):	Comments and further details
3-1	That I can SSH to my nodes.		
3-2	That I have root access to my nodes. This allows me to perform any action on the nodes that I want (install new applications, device drivers, load additional kernel modules, etc).		
3-3	That I can use a single public/private SSH key pair to access my resources on all the different testbeds		
3-4	That I can choose to have Windows installed on my nodes		
3-5	That I can choose to have a specific Linux distribution on my nodes (e.g. latest Ubuntu LTS release)		
3-6	That I can choose to use a custom Linux kernel on my nodes (e.g. with my own performance upgrade patches to the kernel)		
3-7	That my nodes can download and install software from the Internet (e.g. using a package manager)		
3-8	That I can take a binary image of the hard drive of my nodes, and that I can store these for later re-use (so flashing the image back later on)		
3-9	That I can define what a node should automatically do at startup (bootstrap scripts)		
3-10	That during the deployment of my resources over different facilities, that my initial data sets can be automatically loaded to all these resources.		
3-11	That I can allow other people of my work team that are involved in the experiment to use the resources that I have reserved and deployed. I should be able to specify which resources should be shared, and which not.		

3-12	<p>That I can easily use my resources across multiple testbeds using the same common tools. These should be as user-friendly as possible, abstracting the complexity of the underlying infrastructures for me as much as possible. This way I can focus on the experiment itself instead of learning how to work with numerous testbed-specific tools.</p>		<p>Any input regarding which aspects of an experiment the tool should take care of for you are very welcome here (configuring a network node with a specific profile, etc).</p>
3-13	<p><i>If you have any additional requirements regarding resource usage, please insert them here. Create as many new rows in this table as needed.</i></p>		
3-14			
3-15			
3-16			

L.4 Requirements related to orchestrated control of the experiment

In the previous step resources were deployed, and the experiment can manually log in on them and control what they should do. However, when aiming to perform more advanced scenarios, where many resources are included and all of them should be triggered to perform certain task at the appropriate time, more orchestrated experiment control is needed. The corresponding requirements are captured in this section.

	When controlling the execution of my experiment in an orchestrated manner, I require ...	Priority (X or 1-4):	Comments and further details
4-1	That I can define the behaviour over time of a distributed experiment in a single script, which can be started automatically at any desired moment, and will be automatically translated to the corresponding triggers at the nodes at the appropriate time. So e.g. describing in a single script that the 5 client nodes in an experiment should gradually increase their load on the server that they are testing in the experiment. This will be done automatically, without the experimenter login in to these 5 nodes and gradually increasing this load manually.		
4-2	That I can define the behaviour of a distributed experiment in a single script, based on events (e.g. value above threshold). This can be started automatically at any desired moment, and will be automatically translated to the corresponding triggers at the nodes at the appropriate moment. So e.g. describing in a single script that a server should scale up to a VM with more CPU power and RAM when the load of the clients on the server becomes higher than a certain threshold.		
4-3	That the description of the above orchestration is described in a human-readable way. This description should also be uniform across the different testbeds.		
4-4	That the above description of the orchestrated control of the experiment can also include other aspects that will be performed automatically. This includes selection, reservation and deployment of resources; monitoring of the resources and collection of measurement data during the experiment.		
4-5	<i>If you have any additional requirements regarding orchestrated experiment control, please insert them here. Create as many new rows in this table as needed.</i>		
4-6			
4-7			
4-8			

L.5 Requirements related to the results of the experiment (monitoring and measuring data)

The motivation for every experiment is to learn something. For this it is needed that the appropriate monitoring data and experiment measurements are captured. This section grasps the corresponding requirements.

	When capturing the results of my experiment (monitoring and measuring data), I require ...	Priority (X or 1-4):	Comments and further details
5-1	That the internal clocks of resources across multiple testbeds are synchronized very accurately		
5-2	That Fed4FIRE+ makes it easy for me to retrieve and store data that I measured during the runtime of the experiment. This means that it should be easy to store my measurement somewhere in a way that the data is clearly related to the experiment ID, but without needing to establish connections to certain databases manually from within my code, and without needing to know the specific experiment ID that belongs to my current experiment.		
5-3	That by default some common characteristics of my resources are stored automatically for later analyses during experiment runtime (CPU load, free RAM, Tx errors, etc).		
5-4	That for the above monitoring, that I can select and configure how this data should be collected (always at a specified interval, only after a certain event or alarm, define some specific filters, etc).		
5-5	That I can request the monitoring solutions to provide me specific additional on-demand measurements of node characteristics to ease experiment development and debugging		
5-6	That information about external wireless interference during the execution of my experiment is automatically provided for me.		
5-7	That the overall health status of the different testbeds (testbed up or down, has free resources left, etc.) is continuously monitored by the federation, and that in case of issues I am informed of this.		
5-8	That the overall health status of the different testbeds (testbed up or down, has free resources left, etc.) is continuously monitored by the federation, and that in case of issues the corresponding testbeds try to solve them asap.		

5-9	That other aspects related to the successful execution of my experiment are continuously monitored, and that I am automatically informed in case of any errors. Examples are: when a selected resource could not be instantiated, when there is a problem with the interconnectivity between the used testbeds, when a used testbed goes down during the experiment, when there is a sudden peak of wireless interference, etc. This might be important when analysing anomalies in the experiment results.		
5-10	That when an error requiring manual intervention is reported to me as part of the previous step, that I am guided through the process for recovery.		
5-11	That the overhead of any monitoring and measurement tool is minimal. These tools should have a negligible impact on the results of my experiment.		
5-12	That I can store and access my experiment monitoring data and other measurements on a data service on the federation, which is accessible during the experiment (temporarily data storage by the federation)		
5-13	That I can store and access my experiment monitoring data and other measurements on a data service on the federation, which is also accessible after the experiment (archiving of historical data by the federation)		
5-14	That access to my stored data is properly secured. Experiments must be kept confidential if required, the privacy of experiments, data sets and results should be guaranteed.		
5-15	That I can store experiment configurations in order to repeat experiments and compare results of different runs		
5-16	That I can share my stored data with specific others (individuals and/or groups), or even make them publically available		
5-17	That I am made aware if my storage capacity is running out.		
5-18	<i>If you have any additional requirements regarding monitoring and measuring data, please insert them here. Create as many new rows in this table as needed.</i>		
5-19			
5-20			
5-21			

L.6 Requirements related to the interconnectivity of the different testbeds

Fed4FIRE+ facilities are intended to allow experimentation with Future Internet techniques. And because Fed4FIRE+ is a federation of testbeds that enables experiments that included resources from different testbeds, the interconnectivity between the different testbeds is very important. This section enumerates the corresponding requirements.

	When focusing on the connectivity of the resources that will be included in my Fed4FIRE+ experiment, I require ...	Priority (X or 1-4):	Comments and further details
6-1	That resources at different testbeds are interconnected on layer 3 (IP)		
6-2	That resources at different testbeds are interconnected on layer 2, or that such a layer 2 connection can be automatically created for me (in a way that all the underlying technical details are abstracted for me)		
6-3	That I can know the type of interconnections that are available between the testbeds (layer 2 and/or layer 3, NAT or VPN included, dedicated direct link, connected through Géant with or without bandwidth reservation, connected over the public Internet, ...)		
6-4	That I can configure a specific bandwidth on the interconnections between the different testbeds used in my experiment. As long as the links behave as configured, I don't really care what the testbed has to do behind the curtains to implement this (reserve guaranteed bandwidth in case of limited capacity on the interconnecting link, or limit the bandwidth in case of a high capacity on that same link).		
6-5	That my resources are directly reachable, without any network address translation (NAT) or virtual private network (VPN) in between. So actually I require that all resources have a public IPv4 or IPv6 address.		
6-6	That if an issue arises with the interconnection between my used testbeds, that I am automatically informed about this.		
6-7	<i>If you have any additional requirements regarding monitoring and measuring data, please insert them here. Create as many new rows in this table as needed.</i>		
6-8			
6-9			
6-10			

5.3 EXPERIMENT REPORT TEMPLATE





Fed4FIRE+ Experiment Report

Full title of your project Acronym of your proposal (optional)

Date of preparation of your proposal: xx/yy/201x

Version number (*optional*):

Your organisation name:

Your organisation name

Your organisation address:

Your organisation address

Name of the coordinating person:

Name of the coordinating person

Coordinator telephone number:

Coordinator telephone number

Coordinator email:

Coordinator email

(this will be the email address to which the Acknowledgement of Receipt will be sent)



Section A Project Summary

This section provides an executive summary of the experiment objectives, implementation and main results. Remark: The information in this section will be used in public documents and reports by the Fed4FIRE+ consortium. The length of this section is restricted to 1 page.

Section B Detailed Description

This section describes the details on the experiment and provides information as you have been collecting this from your point of view and from your business.

B.1 Concept, Objectives, Set-up and Background

There is no page limit for this section as you are invited to describe the concept, objectives and setup in as much detail as you wish to do. Please also include graphs and figures were needed.

B.1.1 Concept & objectives

Describe in detail the concept and objectives of your experiment.

B.1.2 Set-up of the experiment

Describe in detail the set-up of your experiment. What was the technical design of the experiment? Please include a general overview figure to explain the set-up.

B.1.3 Background / Motivation

Situate this experiment in your business or research activity. Why did you want to execute this experiment? How did this experiment fit within the strategy of your company / institution?

B.2 Technical Results & Lessons learned

Describe in detail the technical results of your experiment and the lessons learned.

There is no page limit for this section as you are invited to describe the concept, objectives and setup in as much detail as you wish to do. Please also include graphs and figures were needed.

B.3 Business impact

Describe in detail how this experiment may impact your business and product development.

B.3.1 Value perceived

What is the value you have perceived from this experiment (return on investment)? E.g. gained knowledge; acquired new competences; practical implementation solutions such as scalability, reliability, interoperability; new ideas for experiments/products; etc.



What was the direct or indirect value for your company / institution? What is the time frame this value could be incorporated within your current product(s) range or technical solution? Could you apply your results also to other scenarios, products, industries?

If no federation of testbed infrastructure would be available, how would this have affected your product / solution? What would have been the value of your product / solution if the experiment was not executed within Fed4FIRE+? What problems could have occurred?

Are there any follow-up activities planned by your company/institution? New projects or funding thanks to this experiment? Do you intend to use Fed4FIRE+ facilities again in the future?



B.3.2 Funding

Was the allocated budget related to the experiment to be conducted high enough (to execute the experiment, in relation to the value perceived, etc.)?

Did you receive other funding for executing this experiment besides the money from the Fed4FIRE+ Open Call (e.g. internal, national, etc.)?

Would you (have) execute(d) the experiment without receiving any external funding?

Would you even consider paying for running such an experiment? If so, what do you see as most valuable component(s) to pay for (resources, support, etc.)?

Section C Open Research Data

This section provides feedback on the actions taken by the proposer in the framework of the Open Research Data (ORD) initiative. If you wish to opt out of this initiative (*even if you previously opted in*), please provide the reasons. If you wish to opt in, please provide DOI of the uploaded dataset, the Final Data Management Plan and all necessary information to show that a complete, publicly accessible dataset of your experiment results and supporting data, has been uploaded in Fed4FIRE+’s chosen repository.

Open Research Data Opt In / Opt Out

<p>Will you provide a complete, publicly-accessible dataset of your experiment results and supporting data, uploaded in Fed4FIRE+’s chosen repository?</p>	<p>YES or NO</p>
<p>For the Answer “NO”:</p>	<p>The experimenter needs to provide reasons why they will not make their experiment data open as part of the proposal. Guidance on opt out reasons can be found in the Open Call Information Document.</p>
<p>For the Answer “YES”:</p>	<p>The experimenter needs upload their data to Fed4FIRE+’s recommended repository (Zenodo - https://zenodo.org/), provide the DOI that Zenodo allocates to identify it, and fill in the following table. This table becomes the Final Data Management Plan, to be submitted with the experiment proposal. Guidance notes are provided in the table. Costs of up to €500 can be claimed by the experimenter for preparation and publishing of ORD.</p>

Instructions for Uploading

Zenodo <https://zenodo.org/> is the recommended Fed4FIRE+ data repository. It is operated by CERN and well used, so it stands a strong chance of long-term archival survival, and it is well-known and easily searchable.

In general, the experimenter makes a zip file of their data and uploads this to Zenodo. Regarding the format, it is up to the experimenter, but the format should be explained within the zip file so that someone else can take the data and use it.

Zenodo is very straightforward to use – the experimenter can create an account (using a standard process), upload the data and give it some description. Some specific notes:

- To upload the data, drag it into the pane or select the files to upload. Make sure you press the “start upload” button on the right, otherwise it will not actually upload the file.
- Specify the type of upload by the radio buttons (most likely this it is a dataset, but there are a few to choose from).

- Zenodo will create a DOI (Digital Object Identifier) for you, which is a unique weblink that you can use to reference the dataset.
- You need a title and some authors – all self-explanatory. If you are an academic and have an ORCID ID, you can put this in the authors section, and it will link to the rest of your ORCID publications (you can also login to Zenodo with your ORCID ID).
- You need a brief description of the data – like an abstract, and some keywords. Each keyword goes in a box on its own - you can't just separate them by commas.
- Re license – if you are happy for anyone to use it for any purpose, “Creative Commons Attribution” is a reasonable choice – this means anyone can use it, as long as you are acknowledged as the author. There are other options as well – if you want to discuss them, please contact slt@it-innovation.soton.ac.uk for help.
- For the funding section, put European Commission (EU) and the Fed4FIRE+ grant number is 732638. This is very important!
- You need to “save” the record (it is suggested that you keep doing this) before publication, and when you are ready to publish, hit “publish”.
- Once you have published, it is not obvious how you see your own published items – you can do this by selecting “Upload” in the main menu bar at the top of the page.

Once upload is completed, please fill in the following table, which comprises the final data management plan. Simply replace the text in the green boxes with your information.

Final Data Management Plan

Section	DMP Category and Question	Final DMP	Fed4FIRE+ Guidance Notes
			Y = mandatory to answer question, O = optional to answer, N/A = not applicable
0	Experiment Information		
	Name of Experiment	Y	
	Names of Experimenters	Y	
	Experimenters' Organisations	Y	
	Fed4FIRE+ Call ID	Y	
	Experiment Start Date	Y	
	Experiment End Date	Y	
	Fed4FIRE+ Testbeds	Y	
	Fed4FIRE+ Sponsor	Y	
	DOI of uploaded dataset	Y	Digital Object Identifier issued by Zenodo after upload.
1	Data Summary		

Section	DMP Category and Question	Final DMP	Fed4FIRE+ Guidance Notes
			Y = mandatory to answer question, O = optional to answer, N/A = not applicable
	What is the purpose of the data collection/generation and its relation to the objectives of the project?	Y	This should be the abstract of experiment from proposal including objectives of collecting the experiment data.
	What types and formats of data will the project generate/collect?	Y	Initially this can be an estimate. In the final DMP this should be a statement of the formats, so it can go into the metadata.
	Will you re-use any existing data and how?	Y	If any external data is anticipated before the experiment starts, state it here. If any external data has been used during an experiment, it must be stated, along with any license terms or stipulations.
	What is the origin of the data?	Y	This is the expected source of the data before the experiment runs, and the actual source of data once the experiment is complete.
	What is the expected size of the data?	Y	Initially this can be an estimate. In the final DMP this should be the actual size of the data.
2	FAIR data		
2.1	<i>Making data findable, including provisions for metadata</i>		
	Are the data produced and/or used in the project discoverable with metadata, identifiable and locatable by means of a standard identification mechanism (e.g. persistent and unique identifiers such as Digital Object Identifiers)?	Y	Initially, this should be a statement committing that the experiment data will be discoverable. When the experiment is complete, the experiment data's Digital Object Identifier (DOI) and metadata should be cited. Fed4FIRE+'s repository of choice, Zenodo, allocates a DOI at upload time, and allows keywords to be entered into a form. These keywords will form part of the metadata that allow the data to be discoverable.
	What naming conventions do you follow?	Y	Initially this can be optional, although it is recommended to think of the naming conventions before the data is collected. After the experiment, this should cite the naming conventions used.
	Will search keywords be provided that optimize possibilities for re-use?	Y	This should always be YES - there will be or are keywords for search terms. The keywords should be stated here.
2.2	<i>Making data openly accessible</i>		

Section	DMP Category and Question	Final DMP	Fed4FIRE+ Guidance Notes
			Y = mandatory to answer question, O = optional to answer, N/A = not applicable
	What methods or software tools are needed to access the data?	O	If there are any special tools or methods needed to access the data (e.g. commercial software tools that can open the data's format), state them here.
	Is documentation about the software needed to access the data included?	O	If software tools are needed, cite the documentation.
	Is it possible to include the relevant software (e.g. in open source code)?	O	If possible, include or cite the software tools (e.g. sourceforge location)
2.3	<i>Making data interoperable</i>		
	Are the data produced in the project interoperable, that is allowing data exchange and re-use between researchers, institutions, organisations, countries, etc. (i.e. adhering to standards for formats, as much as possible compliant with available (open) software applications, and in particular facilitating re-combinations with different datasets from different origins)?	Y	The default position for Fed4FIRE+ is "yes - the data will be (or is) interoperable". This section should be a statement of commitment by the experimenter that the data will be (or is) interoperable.
	What data and metadata vocabularies, standards or methodologies will you follow to make your data interoperable?	Y	Initially, this should be a statement of the formats intended for the data, together with citations of their definitions if applicable (e.g. RFCs etc.). For metadata, the experimenter should cite the anticipated metadata schemas by URL. After the experiment is complete, it should be a statement of the actual formats used, as well as citations to metadata schemas.
2.4	<i>Increase data re-use (through clarifying licences)</i>		
	How will the data be licensed to permit the widest re-use possible?	Y	Initially, this should be a statement of the intended license, which at least must permit open access. Once the experiment is complete, the data must be licensed under terms that permit open access, and the license must be named here. The default license is Creative Commons CC-BY 4.0, and open license that provides attribution of the creator.

Sect-ion	DMP Category and Question	Final DMP	Fed4FIRE+ Guidance Notes
			Y = mandatory to answer question, O = optional to answer, N/A = not applicable
	Are data quality assurance processes described?	O	If any QA procedures are observed, they should be stated - it is in the interest of the experimenter to describe these, as they will help the reusability of the data.
3	Allocation of resources		
	Who will be responsible for data management in your project?	Y	The person responsible for the data management should be named in both the initial and final DMP. This should be the principal experimenter.
4	Data security	N/A	Responsibility of Repository
5	Ethical aspects		
	Are there any ethical or legal issues that can have an impact on data sharing? These can also be discussed in the context of the ethics review. If relevant, include references to ethics deliverables and ethics chapter in the Description of the Action (DoA).	Y	Legal, ethical and data protection issues must to be described in the initial DMP that forms part of the experimenter's proposal before the experiment runs, together with procedures for correct compliance with the applicable laws including the implications of storing the data for the long term in an open repository.
	Is informed consent for data sharing and long term preservation included in questionnaires dealing with personal data?	Y	The experimenter must specify methods for acquiring informed consent in their initial DMP.
6	Other issues		
	Do you make use of other national/funder/sectorial/de partmental procedures for data management? If yes, which ones?	O	If other DMP procedures are used, the experimenter should state them.

Section D Feedback to Fed4FIRE+

This section contains valuable information for the Fed4FIRE+ consortium and describes your experiences by running your experiment on the available testbeds. Note that the production of this feedback is one of the key motivations for the existence of the Fed4FIRE+ Open Calls.

D.1 Resources & tools used

D.1.1 Resources

Describe the testbeds you have been using and specify the resources used.

Please use www.fedfire.eu to get details on the specific testbeds or contact@Fed4FIRE+.eu

Wired networking testbeds		Used?	Specify the type and amount of the resources used
	Virtual Wall (imec)		
	PlanetLab Europe (UPMC)		
	PL-LAB (PSNC)		
	Geant Testbed as a Service (GTS) (Nordunet)		

Wireless/5G/IoT testbeds			
	w-iLab.t (imec)		
	Portable wireless testbed (imec)		
	City of Things Antwerp testbed (imec)		
	NITOS (UTH)		
	Netmode (NTUA)		
	SmartSantander (UC)		
	FuSeCo (FOKUS)		
	PerformLTE (UMA)		
	IRIS (TCD)		
	LOG-a-TEC (JSI)		
	R2lab (Inria)		

OpenFlow testbeds			
	i2CAT OFELIA island		
	NITOS (UTH)		
	Virtual Wall (imec)		

Cloud computing testbed			
	Virtual Wall (including GPUlab) (imec)		
	Exogeni (UvA)		
	Grid5000 (Inria)		

Other			
	Tengu – big data (imec)		



Did you make use of all requested testbed infrastructure resources, as specified in your Open Call proposal? If not, please explain.

What was the ratio between time reserved vs time actually used for each resource? Why does it differ that much (e.g. for interference reasons, other)?

D.1.2 Tools

Describe in detail the tools you have been using, resources used, how many nodes, etc.

<i>Tools</i>	<i>Used?</i>	<i>Please indicate your experience with the tools. What were the positive aspects? What didn't work?</i>
JFed		
JFed command Line (CLI)		
Omni		
OMF		
NEPI		
OML		
<i>Please list below other tools used</i>		

D.2 Feedback based on design/set-up/running your experiment on Fed4FIRE+

Describe in detail your experiences concerning the procedure and administration, set-up, Fed4FIRE+ portfolio, documentation and support, experimentation environment, and experimentation execution and results. This feedback will help us for future improvement.

D.2.1 Procedure / Administration

How do you rate the level of work for administration / feedback / writing documents / attending conference calls or meetings compared to the timeframe of the experiment?

D.2.2 Setup of the experiment

How much effort was required to set up and run the experiment for the first time? Did you need to install additional components before you were able to execute the experiment (e.g. install hardware / software components)?

How do you rate the experience as user that you only had to deal with a single service provider (i.e. single point of contact and service) instead of dealing with each testbed itself?

D.2.3 Fed4FIRE+ portfolio

Was the current portfolio of testbeds provided by the federation, with access to a large set of different technologies (sensors, computing, network, etc.) provided by a large amount of testbeds, sufficient to run your experiment?

Was the technical offering in line with the expectations? What were the positive and negative aspects? Which requirements could not be fulfilled?



Could you easily access the requested testbed infrastructures?

Could you make use of all requested resources at the different testbeds as was proposed in the description of the experiment? If not, how many times did this fail? What were the main reasons it failed (e.g. timing constraints, technical failures, etc.)?

Did you use a lot the combination of resources over different testbeds? Did it all work out nicely? Were they interoperable?

D.2.4 Documentation and support

Was the documentation provided helpful for setting up and running the experiment? Was it complete? What was missing? What could be updated/extended?

Did you make use of the first level support dashboard?

Did you contact the individual testbeds for dedicated technical questions?

D.2.5 Experiment environment

Was the environment trustworthy enough for your experiments (in terms of data protection, privacy guarantees of yourself and your experiment)?

Did you have enough control of the environment to repeat the experiment in an easy manner?

Did you experience that the Fed4FIRE+ environment is unique for experimentation and goes beyond the lab environment and enables real world implementation?

Did you share your experiment and/or results with a wider community of experimenters (e.g. for greater impact of results, shared dissemination, possibility to share experience and knowledge with other experimenters)? If not, would you consider this in the future?

D.2.6 Experiment execution and results

Did you have enough time to conduct the experiment?

Were the results below / in line with / exceeding your initial goals and expectations?

What were the hurdles / bottlenecks? What could not be executed? Was this due to technical limits? Would the federation or the individual testbeds be able to help you solving this problem in the future?

D.2.7 Other feedback

If you have other feedback or comments not discussed before related to the design, set-up and execution of your experiment, please note them below.

D.3 Why Fed4FIRE+ was useful to you

Describe why you chose Fed4FIRE+ for your experiment, which components were perceived as most valuable for the federation, and your opinion what you would like to have had, what should be changed or was missing.

D.3.1 Execution of the experiment

Why did you choose Fed4FIRE+ for your experiment? Was it the availability of budget, easy procedure, possibility to combine different (geographically spread) facilities, access to resources that otherwise would not be affordable, availability of tools, etc.? Please specify in detail.

Could you have conducted the experiment at a commercially available testbed infrastructure?

D.3.2 Added value of Fed4FIRE+

Which components did you see as highly valuable for the federation (e.g. combining infrastructures, diversity of available resources, tools offered, support and documentation, easy setup of experiments, etc.)? Please rank them in order of importance.

Which of these tools and components should the federation at least offer to allow experimentation without funding?

D.3.3 What is missing from your perspective?

What would you have liked to have had within Fed4FIRE+ (tools, APIs, scripts, etc.)? Which tools and procedures should be adapted? What functionality did you really miss?

Which (types of) testbed infrastructures (and resources) would have been very valuable for you as an experimenter within the Fed4FIRE+ consortium?

Is there any other kind of support that you would expect from the federation, which is not available today e.g. some kind of consultancy service that can guide you through every step of the process of transforming your idea into an actual successful experiment and eventually helping you to understand the obtained results?



D.3.4 Other feedback

If you have further feedback or comments not discussed before how Fed4FIRE+ was useful to you, please note them below.

D.3.5 Quote

We would also like to have a quote we could use for further dissemination activities. Please complete the following sentence.

Thanks to the experiment I conducted within Fed4FIRE+ ...