D12.1
POPD Requirement No. 1

Work Package	12
Lead partner	FZJ
Status	Final
Deliverable type	Report
Dissemination level	Confidential
Due date	31.03.2019

Deliverable abstract

The deliverable presents:

- Ethics self-assessment of ENVRI-FAIR
- Principles of personal data protection within the ENVRI-FAIR project
- The personal data protection and ethical guidelines for questionnaires and interviews inside the ENVRI-FAIR project
- Declaration of Conformity with requirements of the General Data Protection Regulation by the Data Protection Officer of Forschungszentrum Jülich as the coordinating institution

ENVRI-FAIR (www.envri-fair.eu) has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 824068

DELIVERY SLIP

	Name	Partner Organization	Date
Main Author	Petzold, Andreas	FZJ	31.03.2019
Contributing Authors			
Reviewer(s)		No review since the document is confidential	
Approver		No approval since the document is confidential	

DELIVERY LOG

Issue	Date	Comment	Author
V 0.1	29.03.2019	Submission of the final document	A. Petzold

TABLE OF CONTENTS

Ethics of Personal Data Processing

Self-Assessment

As the only ethical issue, ENVRI-FAIR involves the collection of personal data. 'Personal data' means information relating to an identified or identifiable natural person.

According to the Ethics Self-Assessment Guidance (Horizon 2020 Guidance — How to complete your ethics self-assessment: V6.1 – 04.02.2019)

ENVRI-FAIR

- **involves** processing of personal data **only** on the level of collecting contact information of participants to meetings and workshops, and within a survey of target groups' needs; participants will be provided in writing with details of what personal information will be processed ant with other relevant information on processing of their personal data as required by General Data protection Regulation (Regulation EU 2016/679);

- **does not** involve
  - processing of special categories of personal data;
  - processing of genetic, biometric or health data;
  - profiling, systematic monitoring of individuals or processing of large scale of special categories of data, intrusive methods of data processing or any other data processing operation that may result in high risk to the rights and freedoms of the research participants;
  - further processing of previously collected personal data;
  - publicly available data;

- **does not** plan to
  - export personal data from the EU to non-EU countries;
  - import personal data from non-EU countries into the EU.

Confirmation on Personal Data Collection

The ENVRI-FAIR coordination confirms that in the course of the project

- only personal data such as contact details will be collected;
- any personal data other than contact details will **not** be collected.

Declaration of GDPR Compliance

Forschungszentrum Juelich GmbH (FZJ) as the coordinating institution declares that FZJ has implemented measures that correspond to the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), hereinafter the "GDPR".

These measures include:

- Secure handling of personal data with which we can come into contact as a part of the provision of services for you.
- Ensuring the continuous trustworthiness, integrity and availability of the information systems we use to provide services for you.
- The ability to perform timely recovery of the availability of personal data processed as a part of services for your company and access to them in the event of a physical or technical security incident in our information systems.
- In our organisation a set process for informing your company in the event of a breach of the protection of personal data with which we could come into contact as a part of the provision of services for you.
- The ability, through appropriate measures, to respond to a request for the exercise of rights by a personal data subject (Chapter III of the GDPR).
- A set process of regular assessment of the effectiveness of technical and organisational measures to ensure the security of personal data processed in our company.
- Constant Training & Awareness initiatives on data security as well trained employees are vital to the continued compliance of the GDPR.

We take the privacy and security of individuals and their personal information very seriously and take every reasonable measure and precaution to protect and secure the personal data that we process. We have robust policies and procedures in place to protect personal information from unauthorised access, alteration, disclosure or destruction and have several layers of security measures.

If you have any questions how we met the demands of the GDPR, please contact the appointed Data Protection Officer.

Note: The original Declaration of GDPR Compliance signed by the Data Protection Officer of Forschungszentrum Juelich GmbH is part of this Deliverable.

Data Protection in ENVRI-FAIR

Data Protection Management

Data Protection Officer:

Forschungszentrum Juelich GmbH DPO Frank Rinkens, email DSB@fz-juelich.de

The DPO of Forschungszentrum Juelich GmbH ensures the proper execution of implemented measures to comply with GDPR requirements.

ENVRI-FAIR Data Manager:

ENVRI-FAIR uses the open-source Redmine environment for storage of project-related contact information of participants and project-related documents. The system is a password-protected and secured system for project data storage. The access is controlled, and can be specified for specific times. The system is hosted at Forschungszentrum Juelich GmbH.

The Redmine system is administrated by the ENVRI-FAIR data manager

Ulrich Bundke, email u.bundke@fz-juelich.de

Forschungszentrum Juelich GmbH ensures the required ENVRI-FAIR related file keeping of

- detailed information on the procedures for data collection, storage, protection, retention, an destruction, and confirmation that they comply with national and EU legislation;
- detailed information on the informed consent procedures in regard to the collection, storage, and protection of personal data;
- templates of the informed consent forms and information sheets.

Guidelines for ENVRI-FAIR Questionnaires

The ENVRI-FAIR Data Management plan and the ethical guidelines state the following procedure for conducting a questionnaire. The issues related to data storage are bolded below.

Before making any questionnaires, consider the following requirements:

1. Collection of any private data (including e.g. opinions, names, positions, etc.) is to be avoided if not useful for the purpose of the study. Make sure that all information you collect are strictly required for the actions described in the Description of Action document of the Grant Agreement with the EC.

2. If such information is needed, the target of the study must be informed before the data collection about

a. collected information,
b. why it is needed,
c. how the targets were selected,
d. who has access to the data,
e. any anonymization scheme (if any) is used,
f. how the data will be analysed,
g. how the target and either agree on disagree on the terms,
h. how the access to the data will be controlled,
i. how long and where the data will be stored, and
j. how long it approximately takes to answer the questionnaire.

This is best done by including header information on your questionnaire.

3. The data retention must be carefully considered, and if the raw data sets (answers) do not need to be stored, they must be destroyed after use. We require that all personal information is destroyed latest on the project end, preferably immediately after the conclusions of the study are finalized.

4. You must indicate a responsible person for the questionnaire who is responsible that the material is adequately stored and handled. He or she is also responsible on the access control, data storage and on destruction of personal information.

5. Data storage must be adequate to the level of sensitivity of the data. Use of separate protected areas in the common Redmine virtual platform can be arranged – please contact the project office if needed.

6. Access control of the data must be adequate and clearly defined, including access policies in the long-term storage (if needed).

7. You MUST fill any registration information legally required by your country of operations regarding the storage of personal information. This is YOUR responsibility.

8. Details will be specified in the DMP.

List of Acronyms

BEERi	Board of European Environmental Research Infrastructures - is an internal advisory board representing the needs of environmental Research Infrastructures
CA	Consortium Agreement - Legal contract between the ENVRI-FAIR beneficiaries
DL	Deliverable / Deadline
DMP	Data Management Plan
DMT	Data Management Team
DoA	Description of Action
DPO	Data Protection Officer
EB	Executive Board - supervisory body for the execution of the Project
EC	European Commission - is the executive body of the European Union responsible for proposing legislation, implementing decisions, upholding the EU treaties and managing the day-to-day business of the EU
ESFRI	European Strategy Forum on Research Infrastructures
GA	(1) Grant Agreement - Contract between Coordinator and Commission (2) General Assembly - GA is the ultimate decision-making body of the consortium
GDPR	General Data Protection Regulation
PM	Person Month
PMT	Project Management Team
POPD	Protection of Personal Data
PWG	Policy Working Group
RI	Research Infrastructure
ToR	Terms of Reference
WP	Work Package

JÜLICH
Forschungszentrum

DECLARATION OF CONFORMITY WITH REQUIREMENTS OF REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL OF 27 APRIL 2016 ON THE PROTECTION OF NATURAL PERSONS WITH REGARD TO THE PROCESSING OF PERSONAL DATA AND ON THE FREE MOVEMENT OF SUCH DATA, AND REPEALING DIRECTIVE 95/46/EC (GENERAL DATA PROTECTION REGULATION)

To whom it may concern, July 2018

We declare that our company has implemented measures that correspond to the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), hereinafter the "GDPR".

These measures include:

- Securehandling of personal data with which we can come into contact as a part of the provision of services for you;
- Ensuring the continuous trustworthiness, integrity and availability of the information systems we use to provide services for you;
- The ability to perform timely recovery of the availability of personal data processed as a part of services for your company and access to them in the event of a physical or technical security incident in our information systems;
- In our organisation a set process for informing your company in the event of a breach of the protection of personal data with which we could come into contact as a part of the provision of services for you;
- The ability, through appropriate measures, to respond to a request for the exercise of rights by a personal data subject (Chapter III of the GDPR);
- A set process of regular assessment of the effectiveness of technical and organisational measures to ensure the security of personal data processed in our company.
- Constant Training & Awareness initiatives on data security as well trained employees are vital to the continued compliance of the GDPR

We take the privacy and security of individuals and their personal information very seriously and take every reasonable measure and precaution to protect and secure the personal data that we process. We have robust policies and procedures in place to protect personal information from unauthorised access, alteration, disclosure or destruction and have several layers of security measures

If you have any questions how we met the demands of the GDPR, please contact the appointed Data Protection Officer.

Frank Rinkens
CISO/IT-Sicherheitsbeauftragter, CISM
& DPO/Datenschutzbeauftragter
Forschungszentrum Juelich GmbH/Projektträger Jülich
DSB@fz-juelich.de