FIT4REUSE

Safe and sustainable solutions for the integrated use of non-conventional water resources in the Mediterranean agricultural sector

Deliverable: D1.3

Work Package: WP1

Due date of deliverable: 31 December 2019
Actual submission date: 31 December 2019

FIT4REUSE is part of the PRIMA Programme supported by the European Union.

The PRIMA programme is supported under the Horizon2020, the European Union's Framework Programme for Research and Innovation.

FIT4REUSE is part of the PRIMA Programme supported by the European Union.

The PRIMA programme is supported under the Horizon2020, the European Union's Framework Programme for Research and Innovation.

DOCUMENT INFORMATION

Deliverable	**Number**	1.3	**Title:**	Protocol on ethical principles for the management of personal data		
Work Package	**Number**	1	**Title:**	Project Management and Coordination		
Due date of deliverable	**Contractual**		31/12/2019	**Actual**	31/12/2019	
Version number	**3**					
Format	**Word**					
Creation date	15/11/2019					
Version date	31/12/2019					
Type	☒ **R**	☐ **DEM**		☐ **DEC**	☐ **OTHER**	
Dissemination Level	☒ **PU Public**			☐ **CO Confidential**		
Target groups (if public)	☒ Scientific Community (higher education, Research)		☒ Industry		☒ Civil Society	
	☒ General Public		☐ Policy makers		☐ Medias	
	☐ Investors		☒ Other			
Responsible authors	**Name:**	Daria Zizzola	**E-mail:**	daria.zizzola2@unibo.it		
	Partner:	UNIBO				

FIT4REUSE is part of the PRIMA Programme supported by the European Union.

The PRIMA programme is supported under the Horizon2020, the European Union's Framework Programme for Research and Innovation.

Rights	**Copyright "FIT4REUSE Consortium".** **During the drafting process, access is generally limited to the FIT4REUSE Partners.**
Brief Description	The Protocol on ethical principles for the management of research data contains measures to guarantee the respect of ethical principles in all research activities, especially those related to the collection, treatment and conservation of personal data of external participants recruited within the consultation sessions organized within T8.6. The Protocol has been designed in compliance with National and EU legislation on ethical issues as well as provisions foreseen in the European Code of Conduct for Research Integrity.
Keywords	Ethics, Personal Data, Management of research data

Version log Revision history

Rev. No.	Issue Date	Modified by	Comments
1	12/12/2019	Antonia Lorenzo (BIOAZUL)	Comments and revisions of the content
2	31/12/2019	Daria Zizzola, Stevo Lavrnić. Attilio Toscano (UNIBO)	Revision following latest comments from the partners

TABLE OF CONTENTS

LIST OF TABLES

EXECUTIVE SUMMARY

This deliverable contains the information and documents required by EU and national regulations to ensure compliance with ethic requirement in the management of personal data as:

- Confirmation that beneficiaries have appointed a Data Protection Officer (DPO) and that the contact details of the DPO are made available to all data subjects involved in the research. For beneficiaries not required to appoint a DPO under the General Data Protection Regulation (GDPR) a detailed data protection policy for the project must be kept on file and submitted to the Agency upon request.
- The beneficiary must explain how all of the data they intend to process is relevant and limited to the purposes of the research project (in accordance with the 'data minimisation' principle).
- A description of the technical and organisational measures that will be implemented to safeguard the rights and freedoms of the data subjects/research participants.
- A description of the security measures that will be implemented to prevent unauthorised access to personal data or the equipment used for processing.
- Description of the anonymysation/pseudonymisation techniques that will be implemented.
- In case personal data are transferred from the EU to a non-EU country or international organisation, confirmation that such transfers are in accordance with Chapter V of the General Data Protection Regulation 2016/679.
- In case personal data are transferred from a non-EU country to the EU (or another third state), confirmation that such transfers comply with the laws of the country in which the data was collected.
- An explicit confirmation that the data used in the project is publicly available and can be freely used for the purposes of the project.
- In case of further processing of previously collected personal data, an explicit confirmation that the beneficiary has legal grounds for the data processing and that the appropriate technical and organisational measures are in place to safeguard the rights of the data subjects.

The following sections contain the details of the DPO for each beneficiary and provide, among others, a description of procedures for the processing of data used for the research, for procedures that will be implemented for the safeguarding the rights and freedoms of the data subjects/research participants, for security measures to prevent unauthorized access to personal data, for the further processing of previously collected personal data.

DISCLAIMER

The PRIMA Foundation is not responsible for any use that may be made of the information this document contains, as it is merely reflecting the authors' view. The authors, the project consortium as a whole and as individual partners, take full responsibility for using the context of this document. The content of this document is not intended to replace consultation of any applicable legal sources or the necessary advice of a legal expert, where appropriate. Therefore, any third party may use the context at its own responsibility and risk.

ABBREVIATIONS

GDPR	General Data Protection Regulation
DPO	Data Protection Officer
INPDP	National Authority for Personal Data Protection

1. General overview

The General Data Protection Regulation (GDPR) provides a common legal framework for all EU Member states and sets guidelines for the collection and processing of personal information of individuals within the European Union (Regulation 2016/679 EU). It applies to all companies processing the personal data of data subjects residing in the Union, regardless of the company's location. The GDPR makes its applicability very clear – it applies to the processing of personal data by controllers and processors in the EU, regardless of whether the processing takes place in the EU or not. The GDPR also applies to the processing of personal data of data subjects in the EU by a controller or processor not established in the EU, where the activities relate to: offering goods or services to EU citizens (irrespective of whether payment is required) and the monitoring of behavior that takes place within the EU. Non-EU businesses processing the data of EU citizens also have to appoint a representative in the EU.
The GDPR has also an impact on research activities. International research consortium must implement a data processing compliant with the GDPR (artt. 6, 7, 8, 9, 13, 14 of the GDPR), releasing a proper information sheet and consent form.

2. Processing of data

2.1 Data Minimization principles

The data minimization principle is set out in art.5 (1) (c) of the GDPR, and it states that:

"1. Personal data shall be:
(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation)"
The data processing is done within the research activities framework and after the collection of data subject's consent.
A fundamental principle underpinning the whole research activity is the respect for the welfare (health and safety) of the participants who take part in the work, and this principle will over-ride all other considerations when the work is executed. Other principles are: privacy, anonymity and confidentiality, fairness, equity, justice, and social responsibility.

The research will be conducted ensuring respect for the participants and their dignity, protecting their values, rights and interests and fair distribution of research benefits and burden. As a general principle, benefits are maximized and harm/risks minimized.

Each Partner involved in the use of personal data for research purposes will be responsible for monitoring and implementing the necessary measures to ensure compliance with National and EU legislation concerning the ethical issues. Ethical standards will be applied in alignment with Horizon 2020.

Here below the specific procedures which will be followed are described.
This document provides guidance for discussion of the ethics issues involved in the project and how they will be dealt with. There are two key aspects:
- A) Human beings
- B) Personal Data

A) HUMAN BEINGS
This proposal involves **human participants** as **volunteers to be recruited for social sciences research.** The participants will be able to give informed consent, they will not be vulnerable individuals or groups, children/minors, patients neither healthy volunteers for medical studies.
Basic principles for human subject research are considered:
- Voluntary informed consent: Participation in research should be based on voluntary informed consent
- Minimum risks: Risks to individuals should be minimised
- Benefits outweigh risks: Benefits from the research should outweigh any risks
- Fair distribution of risks and benefits: Benefits and risks should be fairly distributed across populations
- End participation at any time: Subjects should be free to end participation at any time

Details of recruitment, inclusion and exclusion criteria and informed consent procedures.
Three methodologies employed in the proposal involves human participants: (a) Stakeholders' meetings, (b) Interviews with key stakeholders and (c) Survey to individuals.

(a) Stakeholders' meetings

Stakeholders' meetings could be conducted through formal workshops, under the Water Reuse days, or organized locally. They aim at englobing together representatives from the local administration (policy-makers), local associations (NGOs involved in water bodies); water technologies experts, and general public (i.e., citizens).
Meetings will take place in FIT4REUSE territories as well as during the Water Reuse days (WP8).
The information gathered will be utilized for Task 7.1, 7.2, 7.3, and Task 8.5.

(b) Interviews with key stakeholders

Interviews with key stakeholders will be conducted locally. The interviews aim to collect qualitative data regarding the assessment of environmental, costing and social impacts; as well as about the policy framework of each territory assessed. The interviews will be done with representatives from the local administration (policy-makers), local associations (NGOs involved in water sustainability, water technologies and water policy frame, neighbours' associations) and involved stakeholders (e.g., shareholders, consumers, users).
Interviews will take place in FIT4REUSE territories as well as during the Water Reuse days (WP8). The information gathered will be utilized for Task 7.1, 7.2, 7.3, and Task 8.5.

(c) Survey to individuals

Survey to individuals aim to collect quantitative data on how the consumption patterns of consumers may change as a response to transformative learning when engaging in water-reuse or territorial linkages with the FIT4REUSE activities.
Whenever possible, the surveys will be launched within the Water Reuse Forum (WP8)
The information gathered will be utilized for Task 7.1, 7.2, 7.3, and Task 8.5.

RECRUITMENT PROCESS:
Potential participants will be identified as follows:
- Screening of the stakeholders involved in water reuse-economies or affected by the FIT4REUSE project due to territorial conditions;
- *Snowball sampling* (sampling technique where existing study subjects recruit future subjects from among their acquaintances);
- direct contacts of FIT4REUSE members;
- indirect contacts through local stakeholders (e.g., local researchers, associations, businesses);
- through promotion of the event in local institutions and businesses.

Each technique will last from 30-180 minutes and will be performed in a neutral territory.

INFORMED CONSENT PROCEDURES:

An informed consent form will be provided to each participant prior to any of the three techniques described. The data collection technique will not start until the participants has fully understood, agreed and signed the form.

DOCUMENTS:
The following documents will be provided in English and local language to each participant.
- Information sheet
- Informed consent form
Information sheet and consent form templates are included to this deliverable as annexes.

INCLUSION AND EXCLUSION CRITERIA:
Targeted interview participants will be adult humans (>18 years) able to give informed consent that are not considered as a vulnerable individual.
As participants will be recruited according to their involvement in water reuse interest or territorial link (as consumers, promoters, policymakers, practitioners, farmers, etc.) to accomplish with the research objectives, a strategy to avoid discriminatory practice will be considered in the recruitment. When multiple potential participants have the same involvement in water reuse interest or territorial (i.e., have the same interest for research purposes), recruitment of participants will be performed in an equitable way, in terms of gender, age and nationality.

B) PERSONAL DATA
Data collection:
As indicated in the informed consent, participants will be informed about the purpose and procedure of the interview, and will voluntarily agree on:
- The confidentiality of their identity: "Unless you give us permission to use your title, and / or quote you in any publications that may result from this research, the information you tell us will be confidential."

Data processing:
The processing of personal data will be carried out only for the specific purposes of the project: the data collected will not be disseminated in any way or disclosed to third parties that are not formally involved in the research activities. Regarding the data processing, both with and without using electronic means, the most rigorous security measures will be adopted to ensure the integrity, confidentiality and control of them, in accordance with the provisions of the Italian Personal Data Protection Code and with rules established by the Data Protection Authority of each country where data collection take place.

Secondary data:
Publicly available data sources will be prioritized during the execution of this research. Public data will be properly cited, as essential scientific practice. In case data are obtained from private sources, f.i. some environmental figures which would need the acquisition of a specific database (such as Ecoinvent database within the private software SimaPro), they will be

treated according to European and national legal provisions applying in every single case and according to confidentiality and security obligations requested by the data source.

2.2 Technical and organisational measures implemented to safeguard the rights and freedoms of the data subjects/research participants and to prevent unauthorised access to personal data

First of all, all the people involved in personal data processing within the research project will be informed before starting research activities and they will receive a detailed information (see art. 13 of the GDPR) and they will explicitly consent to the personal data processing (see Attachment. N. 1). Relating to personal data not obtained directly from the data subject, the information relating to the processing of personal data will not be provided in case of impossibility of the provision to the data subject, or involvement of a disproportionate effort, or the provision is likely to render impossible or seriously impair the achievement of the objectives of that processing, pursuant to Art. 14, par. 5 of the GDPR.
Moreover, the GDPR introduces the principles of accountability, privacy by design and by default. It determines controller and processor's responsibilities and requires the implementation of appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation (art. 23-25 and Chapter IV of the GDPR). Controller is responsible for setting out data processing procedures according to the GDPR.
Each Partner participating in the project, as an independent Data controller of the personal data processed in its research is fully compliant with the principles and standards sanctioned by the GDPR and, in particular, implemented organizational and technical measures, pursuant to art. 32 of the GDPR, as detailed below.

2.2.1 Alma Mater Studiorum - University of Bologna (UNIBO)

Alma Mater Studiorum-Università di Bologna has a complex security system for its IT infrastructure (server, personal computer, storage cloud etc.), involving the whole university staff according to Decreto Rettorale n. 271/2009 del 23.02.2009 (Testo unico sulla privacy e sull'utilizzo dei sistemi informatici di Ateneo).
Alma Mater Studiorum-Università di Bologna subscribed the archival system Titulus97, which determines the management, archival, storage rules of the whole administrative paper and digital University's documentation and is the core system on which actions (by design) are implemented to guarantee the protection of personal data.

With regards to personal data protection in the framework of research projects, in particular, Alma Mater Studiorum-Università di Bologna implements organizational and technical security actions:

a) it organizes training courses for administrative staff supporting research teams. Some training workshops involve also researchers in the wider framework of research integrity. These workshops are certified by the University Human Resources Department;
b) it promotes policies to strengthen personal data protection actions (e.g. university staff can access to online resources only after the authentication; passwords must be periodically modifies – every six months – on the basis of an identity management system; authorized personnel only ca access to online resources on the basis of the activities carried out);
c) it promotes security policies through its IT Systems and Services Division (Area Sistemi e Servizi Informatici – CESIA);
d) it provides research teams with IT tools for the data processing and storage. Research teams, for example, can access to university data storage tool in cloud (OneDrive) using the institutional password;
e) it realizes, under the GDPR provisions, a data processing register with risk analysis, impact evaluation and organizational and technical tools to protect personal data. If the data controller considers necessary it, it will contact the national authority dedicated to the personal data protection;
f) it activates, under GDPR provisions, the procedures to inform about data breach and in serious cases can also inform the data subjects involved;
g) it defines the data storage procedures for paper documentation stored in the university archives ("Titulus97") with limited and controlled access;
h) before the submission of a research project, the research team consults the DPO in order to guarantee data minimization and to provide procedures in compliance with the GDPR.

Storage, retention and destruction of data: in compliance with EU and national legislation, research data (files containing questionnaire data for statistical analysis, transcripts of interviews and focus groups, transcripts of field observations, photos, minutes, videos, action diaries, etc.) are stored in computers, laptops, intranet directories, hard-drives, cloud storage systems (i.e. Microsoft OneDrive) of the research institutions accessible through institutional password modified periodically (every 3 months in case of storage of sensitive data), and protected by regularly updated antiviruses.
None of the project data will be left inadvertently available by being left on desks or in unlocked rooms.

All the research materials stored in computers are subjected to back up regularly (according to each institutions' regulations) in order to safeguard them from accidental losses.
As a general principle, all materials that could lead to an identification of the person (e.g., informed consent, names/codes list of participants of the longitudinal study) are stored separately from actual data (questionnaires, transcripts, data files, etc.) and handled by different members of the research team.
All the files containing confidential information and personal details of the research participants are stored in University repository, in compliance with CESIA - IT Systems and Services Division security policies.
In particular the data are password protected (see above), accessible only to authorized the team members (authorized and controlled by the team leader) when they are no more necessary for the research, they are destroyed in according with art. 5 par. 1 letter "e" of GDPR (storage elimination).
The research data are contained on a separate file and do not contain any personal data. Files containing "special categories of personal data (art. 9 GDPR)" will be stored in researchers' laptop, University network folders, cloud systems.
All these resources are managed in compliance with University security policies, regularly subjected to backup procedures, and are accessible only to authorized members of the research teams, protected with University authentication credentials (see above).

According to the art. 37 of GDPR, "the controller and the processor shall designate a data protection officer in any case where:

1. the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
2. the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale […]".

Each Beneficiary of the FIT4REUSE consortium appointed a DPO.

Table 1 - Contact details of DPO for UNIBO

Beneficiary	DPO contact details
UNIBO	privacy@unibo.it - scriviunibo@pec.unibo.it

2.2.2 Marche Polytechnic University (UNIVPM)

Università Politecnica delle Marche (UNIVPM) has a security system for its IT infrastructure to safeguard the rights and freedoms of personal data.
In UNIVPM the processing of personal data for external and research collaborations, such as employment contracts, was approved with **DR n. 594 of 22/05/2019**, according to the EU Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 (GDPR).
Data collection takes place in compliance with the principles of relevance, completeness and non-excessiveness in relation to the purposes for which they are processed. The personal data provided are processed also in compliance with the principles of correctness and transparency, according to article 5 of the GDPR, also with the use of computerized and telematic tools designed to memorize and manage the data, and in any case in such a way to guarantee security, integrity and availability and protecting the confidentiality of the data. The data can be processed anonymously for the performance of statistical and research activities aimed at improving the services offered. Additional information are provided at the following link: https://www.univpm.it/Entra/Privacy/L/1.

Moreover, UNIVPM subscribed the archival system **Titulus** (https://www.univpm.it/Entra/ TITULUS Sistema di Gestione Documentale/L/1), which determines the management, archival, storage rules of the whole administrative paper and digital University's documentation and is the core system on which actions are implemented to guarantee the protection and safe of personal data.
UNIVPM subscribed also the **CINECA IRIS** (Institutional Research Information System). It is an IT solution that facilitates the collection and management of data relating to research activities and products. It provides the user by adjusting and evaluating the tools to monitor the research results, increasing visibility and effectively allocating available resources.
According to the article n° 37 of EU Regulation 2016/679 and following GDPR, UNIVPM has identified as Data Protection Officer (DPO) Dr. Rosalba Sacchettoni, whose contacts are reported in the table below.

Table 2 - Contact details of DPO for UNIVPM

Beneficiary	DPO contact details
UNIVPM	Dr. Rosalba Sacchettoni, Via Oberdan n. 12, 60121 ANCONA, Tel.: 071.2203002, E-mail: rpd@univpm.it, PEC: rpd@pec.univpm.it

2.2.3 National Institute for Environmental Protection and Research (ISPRA)

ISPRA IT infrastructure follows security measures for all data relating to identified or identifiable natural persons (users and third parties, so-called "Interested" subjects pursuant to the GDPR) accessing ISPRA's website. These data may be collected automatically from the same website or inserted voluntarily by the interested parties. More precisely these data can be:

a) Navigation data
Data including IP addresses, users' domain or users' terminals. Furthermore, URI / URL (Uniform Resource Identifier / Locator), time of request to ISPRA's server, size of the response file, the response numeric code (success, error, etc.) and other parameters relating to the operating system and the user's IT environment can be mentioned.
The navigation data, necessary for the use of web services, are also processed in order to obtain anonymous statistical information (most visited pages, number of visitors by time slot or daily, geographical areas of origin, etc.) as well as to check the correct functioning of the services offered.
These data do not persist for more than seven days, except for any need to investigate computer crimes by the judicial authority.

b) Data communicated voluntarily by the user
Optional, explicit and voluntary information can be provided by "interested parties" via emails to Ispra's contact addresses, or private messages to the institutional profiles / ISPRA pages on social media or via forms directly submitted to the Institute website.
Dedicated web pages provide information to users prior to collection of personal data in case those are needed just for limited and specific purposes.

c) Data collected through Cookies
Cookies are small text strings sent by web sites to the user terminal through the browser used to consult those web pages..

ISPRA web site adopts:

- technical session cookies (not persistent), strictly limited to what is necessary for safe and efficient site navigation;
- analytical cookies to collect information, in aggregate form, about the number of users and how they visit the site;
- third-party cookies for sharing content and information through the main social networks or channels (Facebook, Twitter, Instagram).

Whenever the User decides to interact via the social button / widget, or access the Site after having "logged in" through his Facebook, Twitter or Instagram account, some personal information could be acquired by the platform managers of these social networks (for example, the User's visit to the Site). In any case, ISPRA does not have access to data that is collected and processed in full autonomy by the operators of social network platforms and does not use cookies for user profiling.

With regards to **personal data protection in the framework of research projects**, in particular, ISPRA implements organizational and technical security actions.
ISPRA, in its capacity as Data Controller, collects personal data through specific forms available on web site for research activities that can be perfomed both on paper or electronically. Information on data requested for collection and purpose of processing are duly provided.
The processing of personal data is carried out only upon authorization in compliance with the principles of lawfulness and correctness pursuant to art. 5 of the Regulation. While treating personal data ISPRA guarantees confidentiality and security of data processing
Security measures have been set up by the Data Controller, in compliance with the principle of accountability (the so-called Accountability) prescribed by the new EU Regulation, in order to avoid risk of loss, unauthorized access, illicit use and dissemination of the same.

Table 3 - Contact details of DPO for ISPRA

Beneficiary	DPO contact details
ISPRA	avv. Silvia Misirocchi: protocollo.ispra@ispra.legalmail.it - rpd@isprambiente.it

2.2.4 BIOAZUL

BIOAZUL has a security system for its IT infrastructure which includes two servers, personal computers and storage in the cloud in accordance with the provisions of the Regulation (EU) 2016/679 of the European Parliament and the Council, of April 27, 2016.

The data is stored at BIOAZUL servers, with LINUX as operative system and in Dropbox (cloud). The servers are in a locked room. The users need a password to start the server and another password to get into the server files. All users have specific passwords that are changed periodically. Backup copies are done at daily bases in Business Dropbox

account. The data is encrypted locally in the servers. Data which is in hard copies is stored in locked archives.

Within the servers, the data is organised in two folders:

- Documentos de trabajo (all users have access)
- Administración (only the responsible person for the data management has access and the financial officer)

The company WIFI is hidden and with WPA, normally disabled.

With regards to personal data protection in the framework of research projects, in particular, *BIOAZUL* implements organizational and technical security actions as described above, and that are available upon request in the company data protection plan.

Table 4 - Contact details of DPO for BIOAZUL

Beneficiary	DPO contact details
BIOAZUL	alorenzo@bioazul.com (Responsible person assigned as it is not mandatory to assign a DPO due to the type of entity in accordance to art 37 of the GDPR)

2.2.5 ECOFILAE

ECOFILAE has a security system for its IT infrastructure (server, personal computer, storage cloud etc.), involving the whole staff.

With regards to personal data protection in the framework of research projects, in particular, *ECOFILAE* implements organizational and technical security actions:

- it promotes policies to strengthen personal data protection actions (e.g. *ECOFILAE* staff can access to online resources only after the authentication; passwords must be periodically modifies – every six months – on the basis of an identity management system; authorized personnel only ca access to online resources on the basis of the activities carried out);
- in compliance with EU and national legislation, research data (files containing questionnaire data for statistical analysis, transcripts of interviews and focus groups, transcripts of field observations, photos, minutes, videos, action diaries, etc.) are stored in computers, laptops, intranet directories, hard-drives, cloud storage systems (i.e. Dropbox) of ECOFILAE accessible through private password modified periodically (every 3 months in case of storage of sensitive

data), and protected by regularly updated antiviruses. None of the project data will be left inadvertently available by being left on desks or in unlocked rooms.

- all the research materials stored in computers are subjected to back up regularly in order to safeguard them from accidental losses.

As a general principle, all materials that could lead to an identification of the person (e.g., informed consent, names/codes list of participants of the longitudinal study) are stored separately from actual data (questionnaires, transcripts, data files, etc.) and handled by different members of the team.

The data are password protected, accessible only to authorized team members (authorized and controlled by the team leader). When they are no more necessary for the project, they are destroyed in according with art. 5 par. 1 letter "e" of GDPR (storage elimination).

The project data are contained on a separate file and do not contain any personal data. Files containing "special categories of personal data (art. 9 GDPR)" will be stored in team members' laptop, ECOFILAE network folders, cloud systems.

All these resources are managed in compliance with ECOFILAE security policies, regularly subjected to backup procedures, and are accessible only to authorized members of the project teams, protected with ECOFILAE authentication credentials.

Table 5 - Contact details of DPO for ECOFILAE

Beneficiary	DPO contact details
ECOFILAE	nathalie.leroy@ecofilae.fr – nicolas.condom@ecofilae.fr

2.2.6 National Technical University of Athens (NTUA)

The National Technical University of Athens – NTUA is committed to ensuring the security and protection of the personal information processed, and to provide a compliant and consistent approach to data protection. Its current security system for its IT infrastructure is being updated and expanded to meet the demands of the GDPR and the Greek law 4624/2019.

With regards to personal data protection, NTUA implements organizational and technical security actions, aiming to be fully compliant with the GDPR by December 31, 2020. This preparation also applies in the framework of research projects and includes:

- ***Information Audit*** - a university-wide information audit was completed, which identified what personal information is held in each unit, where it comes from, how and why it is processed and if and to whom it is disclosed.
- ***Policies & Procedures*** **-** data protection policies and procedures are being updated to meet the requirements and standards of the GDPR and any relevant data protection

laws. A study has been completed, which includes the above information audit and defines specific steps to be taken in each unit, in order to comply with GDPR's requirements for Data Protection, Data Retention & Erasure, Data Breaches, International Data Transfers & Third-Party Disclosures, and Subject Access Request (SAR). Currently the units revise their procedures and policies according to this study.

- ***Legal Basis for Processing*** - reviewing of all processing activities is being conducted to identify the legal basis for processing and ensuring that each basis is appropriate for the activity it relates to. Where applicable, records of the processing activities are maintained, ensuring that the obligations under Article 30 of the GDPR and Schedule 1 of the Data Protection Bill are met.
- ***Privacy Notice/Policy*** –Privacy Notice(s) are revised to comply with the GDPR, ensuring that all individuals whose personal information is being processed have been informed of why we need it, how it is used, what their rights are, who the information is disclosed to and what safeguarding measures are in place to protect their information.
- ***Obtaining Consent*** - The consent mechanisms for obtaining personal data is revised, ensuring that individuals understand what they are providing, why and how these data are used and give clear, defined ways to consent to the processing of their information. Stringent processes for recording consent are being developed, including the way to withdraw consent at any time.
- ***Data Protection Impact Assessments (DPIA)*** – stringent procedures and assessment templates are being developed for carrying out impact assessments that comply fully with the GDPR's Article 35 requirements, where personal information that is considered high risk, involves large scale processing or includes special category/criminal conviction data is processed.

The Senate of the National Technical University of Athens – NTUA has appointed Dr. Dionysis Rigopoulos as the University's Data Protection Officer on 1st October 2019 – as stipulated in Article 37 GDPR.

Table 6 - Contact details of DPO for NTUA

Beneficiary	DPO contact details
NTUA	Dionysis R. Rigopoulos, Ph.D., drig@central.ntua.gr

2.2.7 National Water Company (MEKOROT)

Mekorot Water Co. LTD is regulated by the Israeli cyber authority and has a security system for its IT infrastructure.
The computer networks have Several layers of protection from the internet including: SIEM managed service, IPS, FW, browsing protection, Secured VPN connection Etc.

User passwords are changed every 90 days, User access to data is on a "need to know" basis.
All systems (computers & Servers) are protected with an Antivirus. Security logs are collected on a regular basis. Security patches are applied on a regular basis.
All data of every user and every system is backed up daily.

With regards to personal data protection in the framework of research projects, in particular, Mekorot Water Co. LTD implements organizational and technical security actions:

1. Mekorot, as a water utility that supplies water only to the gate of municipalities and not directly to the end users in municipalities, never conducts research that includes personal data. Mekorot research involves only technical data.
2. Mekorot has a cyber steering committee headed by the CEO which deals with cyber strategy.
3. The cyber risk is ranked within the top risks short list.
4. Mekorot has a certified CISO.
5. The internal auditor is conducting cyber audits.
6. Mekorot's cyber budget has grown significantly in recent years, and we have implemented many tools and systems (as mentioned above) to protect our networks.

Table 7 - Contact details of DPO for MEKOROT

Beneficiary	DPO contact details
MEKOROT	Zvika Gleichman, zgleichman@mekorot.co.il

2.2.8 Higher Institute for Applied Biological Sciences of Tunis (ISSBAT)

Tunisia has a data protection agency, the National Authority for Personal Data Protection (INPDP). It was created in 2004 pursuant to Law N°. 63 which established the personal data protection regime. In 2007, Decree N°. 3003 defined its organization and functioning. A draft law on the protection of personal data designed to replace Law N°.63 was finally approved in March 2018 and came into force on May 25, 2018. The new law is intended to bring the Tunisian legislation in line with Convention 108 of the Council of Europe for the Protection of Individuals with regard to the Automatic Processing of Personal Data to which Tunisia is party. It requires private data controllers to apply for authorization from the INPDP prior to processing personal data

or transferring it abroad. The INPDP is also mandated to investigate privacy violations and to report those violations to the government. It can also bring violators before the courts.
In addition, the constitution established also human rights as a supreme guiding principle. Article 24, of the Constitution of Tunisian republic of 27 of January 2014, enshrines the right to privacy, making the State responsible for: ''the state protects the right to privacy and the inviolability of the home, and the confidentiality of correspondence, and communications, and personal data.'' Article 32 guarantees the right of access to information, stating: "The state guarantees the right to information and the right of access to information and communication networks."

Tunisia signed of a number of international instruments with Personal Data Protection, including: African Union Convention on Cyber Security and the Protection of Personal Data (Law No 42), The European Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Strasbourg, 28.1.1981), etc.

In December 2014, the Tunisian government revealed plans for the introduction of an electronic ID card and biometric passports by the end of 2016. The new biometric documents (containing each a photograph and scanned fingerprints) would gradually replace the current identity papers.

In Tunisia, a personal data of the public health is well protected by INPDP. In fact, the Section II is carried out to the processing of personal data related to health. According to the Article 14: ''The processing of personal data that reveals, directly or in-directly, the racial and genetic origins, religious beliefs, political, philosophical and trade union belonging or health is prohibited. However, the prohibition provided for the above shall not apply to the processing for which the data subject has given his explicit consent by any means that leave a written trace or if the processing relates to personal data which have become obviously public or if the processing is necessary for historical or scientific purposes or if the processing is necessary for the protection of the data subject's vital interests.''

Public institutions subject to the law include the Presidency, the Prime Minister's office, the judiciary, the parliament, local and regional governorates, as well as all publicly-funded organizations, including Ministry of Higher Education and Research Scientific that receive state subsidies. For example, the Higher Institute of Applied Biological Sciences of Tunis (ISSBAT) is an academic and research state institution currently affiliated to the University Tunis-El Manar under the supervision of the Ministry of

Higher Education and Research Scientific In Tunisia. It was created by Decree N°. 1663 on 4 August 2003. This academic organization underwent the same laws as the public institutions.
ISSBAT makes reference to the National Authority for Personal Data Protection (INPDP) as far as the DPO is concerned.

Table 8 - Contact details of DPO for ISSBAT

Beneficiary	DPO contact details
ISSBAT	The National Authority for Personal Data Protection (INPDP): Inpdp@inpdp.nat.tn

2.2.9 ITUNOVA Teknoloji A.S. (ITUNOVA)

ITUNOVA Teknoloji A S has a modern security system for its IT infrastructure (server, personal computer) in accordance with Turkish Personal Data Protection Law no. 6698.

In October 2018, ITUNOVA achieved certification to the internationally recognised ISO 9001:2015 accreditation, demonstrating its commitment to quality in delivery of our products, services and support. Therefore, ITUNOVA has an established document management system in accordance with ISO 9001 data protection principles to implement data protection controls. Within these guidelines, ITUNOVA has established a management system which ensures the protection of data for personnel and all stakeholders involved in the daily operations (which involves collection, processing, exchange, and storing of personal identifiable information) of this office.

With regard to the technical specifics of our data security, they are as follows:

- **Antivirus**: Trend Micro Worry Free Standard
- **Firewall**: Dell Sonicwall Tz300 AGSS
- **Server**: Physical Server 2012R2 Standard
- **Backups**: Internally, Nas device and externally, on the Microsoft Azure Platform, encoded

While we work closely with the various faculties, institutes and library system of the university, our server is in-house and completely independent. Therefore, only ITUNOVA personnel have access to the information stored within. All employees sign confidentiality agreements upon hiring.

Table 9 - Contact details of DPO for ITUNOVA

Beneficiary	DPO contact details
ITUNOVA	Can Biçer, Projet Yazılım ve Danışmanlık A.Ş. Ağaoğlu My Office F:4/18 Ataşehir/İstanbul-TR Tel : +90 (0216) 250 55 46 Fax : +90 (216) 250 55 56 Mobile: +90 541 685 79 06 canb@projetgrup.com

3. Anonimyzation and pseudonimization

Task within WP7, WP8 and WP9. ISPRA e UNIBO data manager will be the person who will have access to the outcomes of personal data, which will be carefully pseudonymize when data come from the Water Reuse Platform. Data collection derived from the Water reuse days will be managed exclusively by UNIBO and ISPRA team members, where transcriptions will be shared in private folders within the Google Drive folder. Data collection outside mentioned formats will be performed by UNIBO and ISPRA team members and treated with the same confidentiality, exclusively shared with the team members by using private folders, and carefully pseudonymize before any assessment.

4. Transfer to and from non-EU countries

EU data protection rules apply to the European Economic Area, which includes all EU countries and non-EU countries Iceland, Liechtenstein and Norway. When personal data is transferred outside the European Economic Area, special safeguards are foreseen to ensure that the protection travels with the data. These safeguards are defined by the Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation - GDPR).
GDPR applies also for partners based outside the European Union if data are collected in the European Union. It applies also to the case in which data are collected by a subject based in the European Union who transfer them to extra-EU third parties (see Chapter 5 "Transfers of personal data to third countries or international organizations" of the GDPR).

As reported in section 3 personal data will be managed and analyzed by two EU partners: ISPRA and UNIBO. Those institutions will adopt adequate anonymization and

pseudonymization procedures that will ensure that personal data will be rendered anonymous in such a way that the individual is not or no longer identifiable. Therefore, those data will be no longer considered as personal. Partners belonging to the non-EU countries engaged in the project (Israel, Tunisia and Turkey) might receive data only after its anonymization and pseudonymization and thus no personal data will be transferred from EU to non EU-countries.

5. Further processing of previously collected personal data

The research project foresees the possibility to re-use data collected in research projects in similar scientific disciplines, pursuant to Recital 50 of the GDPR, which states that the processing of personal data for purposes other than those for which the personal data were initially collected is allowed where the processing is compatible with the purposes for which the personal data were initially collected, and that, in such a case, no legal basis separate from that which allowed the collection of the personal data is required. In any case, data subjects received specific information in the context of the past scientific research from which such data will be collected.

6. ANNEX

Title of Research Study:

"***FIT4REUSE – sustainability assessment"***

INFORMED CONSENT FORM FOR PARTICIPANTS

You have been invited to participate in a research activity conducted by the Department of Agricultural Sciences of the University of Bologna (Italy) in the frame of the project FIT4REUSE: "Safe and sustainable solutions for the integrated use of non-conventional water resources in the Mediterranean agricultural sector". FIT4REUSE is funded within the PRIMA programme an initiative supported and funded under Horizon 2020, the European Union's Framework Programme for Research and Innovation.

The overall purpose of this activity is to examine the economic, environmental and social impacts of selected non-conventional water resources by adopting a participatory approach based on the organization of selected FIT4REUSE **multi-stakeholder meetings.**

You were selected as a possible participant in this activity because of your expertise and engagement. You are kindly invited to review the information listed below asking for any clarification before deciding whether or not to participate.

- This questionnaire is voluntary. You have the right not to answer any question, and to stop the questionnaire at any time. We expect that the questionnaire will take about half hour.
- You will not be compensated for this questionnaire.
- Unless you provide us with the permission to use your name, title, and / or quote you in any publications that may result from this research, the information you provide us will remain confidential.
- The paper version of the questionnaires will be stored in a secured space (locked under key) until the completion of the project foreseen by 2022. After the end of the project the paper version of the questionnaires will be destroyed.

By signing this form I declare that

- I have understood all the information reported in this form;
- I give permission for storing a paper version of the questionnaire within the conditions stated here above;
- I have requested all the clarification I needed;
- I have been provided with a copy of this form.

Name and signature of the participant Name and signature of the data manager

Date _____ Date _____

Please do not hesitate to contact us for any further information you might need.

Thanking you in advance for you time and availability,

FIT4REUSE, WP7 team, fit4reuse@unibo.it

Title of Research Study:
"***FIT4REUSE – sustainability assessment***"

INFORMATION SHEET FOR PARTICIPANTS

Dear stakeholder,

You are invited to participate in a research study conducted by the Department of Agricultural Sciences of the University of Bologna (Italy) in the frame of the project FIT4REUSE: "Safe and sustainable solutions for the integrated use of non-conventional water resources in the Mediterranean agricultural sector". FIT4REUSE is funded within the PRIMA programme an initiative supported and funded under Horizon 2020, the European Union's Framework Programme for Research and Innovation.

Before you decide whether to take part in the study it is important that you understand the aim of this research as well as the contribution you might provide. Please take time to read the following information and eventually discuss it with others. It is up to you to decide whether or not to take part. If you decide to take part, you will be provided with a copy of this information sheet and requested to sign a consent form. You can change your decision at any time and withdraw from the study without providing a reason. You are welcome to contact us for any additional information you might need.

The overall purpose of this activity is to examine the economic, environmental and social impacts of selected non-conventional water resources by adopting a participatory approach based on the organization of selected FIT4REUSE **multi-stakeholder meetings.** Specifically, you have been invited to contribute to one of this FIT4REUSE **multi-stakeholder meeting**, which is aimed to put together the visions of different stakeholders engaged with non-conventional water resources. The study will involve up to 25 participants, who will participate in two different sessions. The discussions will take approximately 150 min. If you agree to take part to this activity, you will receive all the necessary organizational and logistical information.
The information gained with this research will be used to:
a) complete a screening of the existing water systems (conventional or non-conventional) in your town/region;
b) evaluate the current water reuse legal framework in your town/region;
c) identify the potential effects on citizens.

Please do not hesitate to contact us for any further information you might need.

Thanking you in advance for you time and availability,

FIT4REUSE, WP7 team, fit4reuse@unibo.it