MAGPIE

SMART GREEN PORTS

DELIVERABLE 11.2.
POPD - REQUIREMENT NO. 2

contact@magpie.eu +33 2 35 42 76 12 www.magpie-ports.eu

Funded by the European Union

This project has received funding from the European Union's Horizon 2020 (MFF 2014-2020) research and innovation programme under Grant Agreement 101036594

POPD - REQUIREMENT NO. 2

GRANT AGREEMENT NO.	101036594
START DATE OF PROJECT	1st October 2021
DURATION OF THE PROJECT	60 months
DELIVERABLE NUMBER	D11.2
DELIVERABLE LEADER	POR
DISSEMINATION LEVEL	CO
STATUS	Final
SUBMISSION DATE	22-11-2023
AUTHOR	Arne-Jan Polman, POR, aj.polman@portofrotterdam.com

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101036594.

Modification Control

VERSION #	DATE	AUTHOR	ORGANISATION
V1.0	23-03-2023	A.J. Polman	POR
Final	22-11-2023	A.J. Polman	POR

Release Approval

NAME	ROLE	DATE
A.J. Polman	WP Leader	23-03-2023
M.F. Flikkema	Scientific Coordinator	23-03-2023
A.J. Polman	Project Coordinator	23-03-2023

History of Changes

SECTION, PAGE NUMBER	CHANGE MADE	DATE
		DD-MM-YYYY
		DD-MM-YYYY
		DD-MM-YYYY
		DD-MM-YYYY

Table of Contents

1. Introduction

This document is a follow-up to Deliverable 11.1. As discussed in Deliverable 11.1 H - Requirement No. 1, the MAGPIE project will to a very small extent accumulate personal data from experts and citizens during interviews, regional working groups and focus groups. This document presents information on the processes of data collection, storage, protection, retention and destruction of the accumulated personal data within MAGPIE.

Before going into more detail, it seems a good moment to address a couple of suspected outcomes of the deliverable :

- 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). This must be submitted as a deliverable. This is included in the data management plan D1.7.
- A description of the technical and organisational measures that will be implemented to safeguard the rights and freedoms of the data subjects/research participants must be submitted as a deliverable. This is not applicable.
- Detailed information on the informed consent procedures with regards to data processing must be submitted as a deliverable. This is not applicable.
- Description of the anonymysation/pseudonymisation techniques that will be implemented must be submitted as a deliverable. This is not applicable.
- In case the research involves tracking and profiling, the beneficiary must provide explanation how the data subjects will be informed of the existence of the monitoring and profiling, the possible consequences and how their fundamental rights will be safeguarded. This must be submitted as a deliverable. This is not applicable.
- In case of further processing of previously collected personal data, an explicit confirmation that the beneficiary has lawful basis for the data processing and that the appropriate technical and organisational measures are in place to safeguard the rights of the data subjects must be submitted as a deliverable. This is not applicable.
- All relevant authorisations that the data used in the project is publicly available and can be freely used for the purposes of the project must be submitted as a deliverable. This is included in the data management plan D1.7.

2. Data Collection, Storage, protection, retention and destruction

2.1 Personal data collection in MAGPIE

According to the H2020 Guidance on ethics, personal data is 'any information, private or professional, which relates to an identified or identifiable natural person.' For example: name, address, e-mail, CV, medical records, etc. Sensitive data - e.g. health, sexual lifestyle, ethnicity, political opinion, religious conviction - require specific authorization by the national data protection authority.

Processing of personal data means any operation which is performed on personal data. For example: collection (digital audio recording, video caption), recording, disclosure by transmission (share, exchange, transfer), retrieval and consultation etc.

In MAGPIE no sensitive personal information will be recorded or stored during this project. Therefore, there are no permissions from competent local/national ethic/legal bodies required.

MAGPIE will collect personal information which is usually provided on the experts or stakeholders business cards and which is usually accessible in the public space, or e.g. on their institutions' websites (i.e. information necessary to identify an expert or stakeholder in his or her official or professional role:

- Name
- Country of residence
- Represented institution
- Role in this institution (e.g. General Manager, project manager or similar)
- Email-address

Films and videos are means to disseminate results of MAGPIE to large audiences across Europe. For this reason. The films will be made available on YouTube, and other (social)media, and relevant professional web portals, relevant for the sector. A consent form will be developed to be used for people to be filmed during an interview and for the film to be released on the MAGPIE project website and various social media platforms.

All personal data used for the project will not be saved longer than necessary and will be only used for the purposes agreed in the underlying contracts or data processing agreements.

2.2 Authorisations and mitigation measures

As mentioned in the previous section, MAGPIE will not collect sensitive personal data. Where data is collected from demonstrators, it will be ensured that no details are to be recorded that refer to any individuals of those case studies. However, some of the data are to be treated as confidential and will be accessible only to those involved in this research. We shall therefore protect the data from unauthorized access by taking at least the following steps:

- Files with confidential information will be encrypted so that a key is required for the data files to be accessed. The recovery key shall be shared only among those team members directly involved in the collection and analysis of the relevant files.

- Variables which (when combined) might lead to the identification of demonstrators, will be masked. Masking is the obscuring of information, e.g. through removing or randomizing data in certain fields.
- Access to the data will be restricted through access rights to files and folders (possible in the shared network drive) and through strong passwords.
- Data are circulated between the participants only in so far as this is necessary to fulfil their obligations from the Grant Agreement.
- All files that should not be edited (e.g. raw data files, milestone versions of files) shall be saved as read-only. This way, they cannot be accidentally overwritten or changed.

2.3 Technical data collection in MAGPIE

MAGPIE will collect and generate technical data and information regarding:

- Demonstrator specific key performance indicators, to be finally defined by WP 8 focusing on:
  - Emissions
  - Job creation
  - Autonomy
  - Transport operations.
- Number of attendees to MAGPIE events to generate insight in communication and dissemination reach;
- Website and social media visitors and likes;
- Data on governance approaches.

Most of the data will be collected and generated in the demo cases. In most cases, existing (monitoring) data will be used to describe the situation.

2.4 Data management plan

A data management plan with procedures on data collection, data storage, data protection, data retention, and data destruction will be delivered in month 6 of the project.

Data collection
Throughout the process of data collection, we will keep thorough documentation of all steps taken, such as sources, data cleaning, quality checks, aggregation, and vocabulary used. In addition, any statistical methods used will follow existing methodological standards for the data type in question, and any omission of results is reported and justified. By doing so, we follow the principles of the Netherlands Code of Conduct for Academic Practice). Part of the data will be collected from case studies. In case of confidentiality, contracts will be signed outlining the data collected, the confidentiality of these data, the goals of processing these data, and ownership of these data.

Data storage

All information that will be collected will be stored on partners' protected data storage systems. Where sharing of the data across partners is required, we will make use of Sharepoint, a cloud storage offered hosted by MAGPIE partner TNO.

Data protection and intellectual property

The project aim will be to make as many outputs as possible freely available and accessible. However, MAGPIE appreciates that data, knowledge and other intellectual property which come from participants who are in the non-governmental or university sectors cannot be revealed too early in their development without risking original ideas being exploited by outsiders. Disclosure of knowledge can therefore be a sensitive issue. It will be essential to understand current legislation and protocol, and to be able to adapt procedures to safeguard those whose knowledge needs protection, including local actors whose knowledge and experience water quality protection and its management might be tapped during the various research activities.

Data retention

Following the Netherlands Code of Conduct for Academic Practice, all research data underlying publications will be retained for ten years. The data that can be made accessible to other researchers (i.e. not marked as not shareable in the contracts) will be made available online through a repository. In the data management plan the choice for the repository will be indicated. We are well aware of a possible conflict between the need of data retention and the wish to erase personal data. In such cases, the project management team will decide which position should gain priority.

Data destruction

All data and contextual information that is not retained for purposes of verification and reuse will be destroyed. To destroy the data, files will be deleted from the computers they are on. However, as this only removes the reference to the file and not the file itself, specialized software will be used to completely delete the files from the hard drives. Data are not planned to be stored on other media such as thumb drives or CDs unless this is needed for transfer – however, in the event of data being on such media, these devices will be destroyed to ensure destruction of the data and to mitigate the risk of data breaches.

2.5 Legislation

The consortium's and its partners' data protection policies are fully compliant with EU regulations and partner countries' national rules, including the Regulation (EC) N 45/2001 of 18 December 2000 and EU Regulation 2016/679 (the General Data Protection Regulation) on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

Moreover, partners comply with the individual national law towards data protection.

Throughout the entire research process, MAGPIE will follow national and EU legislation. Such legislation includes the European Convention on Human Rights, the Charter of Fundamental Rights of the European Union, and the Horizon 2020 rules for participation and dissemination. In addition, we will follow the Netherlands Code of Conduct for Academic Practice, ensuring that our research data is authentic, verifiable and durable.

2.6 Consent procedures and data protection policy

Detailed information on the informed consent procedures that will be implemented in regard to the collection, storage and protection of personal data must be obtained on request.

The data protection policy of the consortium and this detailed statement will be presented to the public on the project website for free download. Each of the contacted stakeholders will be provided with an electronic copy (email) or a printout of this data protection policy upon his or her request. Each of the experts and stakeholders will be informed and asked for her or his prior written consent (e.g. by mail) before any data are stored in any of the partners' data bases. Without any prior written consent, these data will not be stored. Stored data will be only used for the purpose of this project and exchanged only between the partners as far as this is necessary for the implementation of this project.

In the case of communication with third parties, a reference to this policy will be made. The data protection policy will also contain a process for data subjects. This also mentions the point of contact for data subjects to carry out their rights.

2.7 Final Statement

All partners have been involved in the compilation and review of this detailed information and are committed to thoroughly implement the data management policy presented in this report. All partners confirm that they comply with national and EU legislation and the procedures for data collection, storage, protection, retention and destruction of personal data. This is also indicated in the Grant Agreement and Consortium Agreement.