Data Management Plan (DMP)

Deliverable 6.2

Work package: **WP6**
Dissemination level: **PU**
Lead partner: ITHACA S.r.l.
Authors: **Fissore V., Monteforte F.**
Due date: **30 / 04 / 2026**
Submission date: **15 / 05 / 2026**

The OVERWATCH project has received funding from the Horizon Europe call "HORIZON-EUSPA-2021", topic HORIZON-EUSPA-2021-SPACE-02-52, under agreement No. 101082320

Deliverable	**Data Management Plan**
Deliverable No.	D6.2
Work Package	6
Dissemination Level	PU
Nature[1]	R
Author(s)	Fissore V. (ITHACA)
Co-Author(s)	Dequal L., Monteforte F. (ITHACA)
Date	15/05/2026
Status	Second issue
Version	1.2

Deliverable abstract	The Data Management Plan defines how the different types of data are managed within the 6 WPs of the OVERWATCH project. This is the second issue of the documents and it contains updates until project closure.

[1] Nature of the deliverable: **R** = Report, **P** = Prototype, **D** = Demonstrator, **O** = Other

Table of Content

Tables

Document revision history

Version	Date	Modification reason	Modified by
1	03/04/2023	First issue	Vanina Fissore, Luciana Dequal, Gianmarco Pignocchino, Federico Monteforte.
1.1	31/05/2023	Revised version	Vanina Fissore, Luciana Dequal, Federico Monteforte.
1.2	30/04/2026	Second issue	Vanina Fissore, Federico Monteforte.

List of authors, contributors and reviewers

No.	Name	Role	Organisation
1	Vanina Fissore	Author	ITHACA
2	Luciana Dequal	Co-author	ITHACA
3	Gianmarco Pignocchino	Co-author	ITHACA
4	Federico Monteforte	Co-author	ITHACA
5	Elizabeth A. Nerantzis	Reviewer	ALPHA

Abbreviations

AI	Artificial Intelligence
AR	Augmented Reality
CA	Consortium Agreement
CEMS	Copernicus Emergency Management Services
CH	Chapter
D	Deliverable
DM	Data Manager
DMP	Data Management Plan
EGNSS	European Global Navigation Satellite System
EO	Earth Observation
FAIR	Findable, Accessible, Interoperable, Re-Usable
GA	Grant Agreement
GDPR	General Data Protection Regulation
IPR	Intellectual Property Right
SFTP	Secure File Transfer Protocol
TRL	Technology Readiness Level
WP	Work Package

Executive Summary

The present deliverable is the second version of the Data Management Plan (DMP) of the OVERWATCH project. This version updates the previous first issue dated 30/04/2023, reporting updates related to the 3 years of project life on data management policy - i.e., collecting and sharing procedures - including a description of the datasets used considering how these have been collected, processed or generated in all work packages during the 42 months of the OVERWATCH project. It contains all guidelines agreed by partners to allow data to be FAIR – Findable, Accessible, Interoperable and Re-Usable. The document can be also considered as a list of data that have been adopted during the project lifetime.

The deliverable has been prepared with the collaborative work among the Coordinator and the Consortium Partners involved in data collection, production, and processing.

1. Introduction to OVERWATCH project

OVERWATCH aimed to develop an intuitive and decentralised crisis management system to support disaster response across different phases of an emergency. Leveraging EGNSS and Copernicus services, the project integrated EO and drone data through advanced AI techniques to provide accurate and actionable information. The system included a backend platform for data management and an AR-based interface offering an immersive overview of the crisis scenario. The solution was validated through demonstrations in two different countries.

2.OVERWACTH Consortium

After partner beneficiary termination of ROBOTTO (at M21), the OVERWATCH project consortium went from 10 to 9 partners from five different countries (Italy, Portugal, Poland, Germany, Denmark), consisting in the following members:

Beneficiary no.	Acronym	Designation	Country
1	ITH	ITHACA S.R.L.	IT
1.1	LINKS	FONDAZIONE LINKS - LEADING INNOVATION & KNOWLEDGE FOR SOCIETY	IT
2	ISQ	INSTITUTO DE SOLDADURA E QUALIDADE	PT
3	CBK	CENTRUM BADAN KOSMICZNYCH POLSKIEJ AKADEMII NAUK	PL
4	ENG	ENGINEERING - INGEGNERIA INFORMATICA SPA	IT
5	ROBOTTO	ROBOTTO CO APS	DK
6	INESCTEC	INESC TEC - INSTITUTO DE ENGENHARIADE SISTEMAS E COMPUTADORES, TECNOLOGIA E CIENCIA	PT
7	HOLO	HOLO-INDUSTRIE 4.0 SOFTWARE GMBH	GE
8	CINAMIL	EXERCITO PORTUGUES	PT
9	ALPHA	ALPHA CONSULTANTS S.R.L.	IT

Table 1 – OVERWATCH Consortium

3. Aims of the Deliverable

The present Data Management Plan (DMP) outlines how the data are handled throughout the lifecycle of the OVERWATCH project in all the work packages, from their collection/generation up to their storage and archive.

The DMP defines the data management methodology in compliance with the FAIR data principles, i.e., to assure that the research data are Findable, Accessible, Interoperable and Reusable. Moreover, the DMP identifies the way the data will be stored and preserved along the project lifetime.

This deliverable can also be considered as a list of data that have been adopted within the 42 months of the project, and, consequently, as a living document that has been updated and adjusted, in line with the progress of the project, and flowing into this final version provided at M42 (end of project).

All partners have been involved in the updating of the DMP, in accordance to the Grant Agreement (GA) [RD04] and Consortium Agreement (CA) [RD05], and have been supervised by the Data Manager (DM), Mr. Monteforte Federico (federico.monteforte@ithaca.earth), appointed by ITHACA. The DM coordinated the data management of the Project to assure usability, accountability and quality of the data and valorise them.

Also, as per GA, the DM has been supported by the Ethics and Security Manager which have as objectives to oversee that all activities such as gathering, processing and analysing sensitive data, ensure that the established procedures are followed and fulfil all obligations with regard to confidentiality while ensuring the compliance with the regulation including the General Data Protection Regulation (GDPR).

The DMP has been prepared considering the template provided by the official Horizon Europe Data Management Plan Guidelines and adapted based on the specificity of the project. The following structure has been accordingly defined:

- OVERWATCH Data Summary
- Description of FAIR data characteristics
- Allocation of resources
- Data Security
- Ethics

4. OVERWATCH Data Summary

All OVERWATCH datasets are reported in the current chapter. The list of OVERWATCH datasets has been collected since the beginning of project activities in a dedicated form made available by PC, namely the Data Summary Form (excel file) to all partners, stored in the OVERWATCH Microsoft Team [RD007]. Partners providing the datasets fill them in and keep it updated when new datasets are collected or implemented within the project's activities.

The Data Summary Form is structured considering all six Work Packages (WPs), where WP2-WP3-WP4 have been grouped as they are the technical WPs.

Moreover, the different types of data produced by the project can be grouped across the following identified categories:

- Documentation material: transcripts and agendas of meetings, recordings of meetings, videos and photos, reports.
- EO / EO-derived data: i.e. satellite data, raster and vector data, open datasets, etc..
- Drone images and videos.
- Location data: GNSS, others.

The tables here reported are taken and pasted from the Data Summary Form and have been organized as follows. For each row we have the following mandatory information:

• Dataset Name: the name of the dataset
• Data Type: see previous categorization
• Original Data Format: e.g. Jpeg, TIFF, pdf

• Data Provider: e.g. Copernicus, CERN, etc.
• Data source: e.g. Sentinel-1 • Data Access rights: only for internal usage, public, etc.
• Data access right: public or internal

Whenever available, or applicable, the following optional information are collected:

• Spatial resolution
• Temporal resolution
• Temporal coverage available
• Data Availability
• Metadata Available

Detailed information is provided only for those WPs for which updates have been introduced with respect to Issue No. 1 of the present document. In particular, only newly collected or implemented datasets are reported.

4.1. WP 1

No new updates with respect to Issue n.1 of the present document have been implemented.

4.2. WP 2 – Wp3 – WP 4

These WPs are devoted to the definition of the system architecture, to the development of the technological modules that will constitute the OVERWATCH system as a whole, (i.e., EO mapping, Drone mapping, AR Holographic interface, Fallback communication network), and to their final integration.
Table 2 provides the list of new datasets introduced.

DATASET NAME	*DFATA TYPE*	*DATA FORMAT*	*DATA PROVIDER*	*DATA SOURCE*	*ACCESS RIGHT*
Custom User GeoTIFF images (e.g. aerophotos)	raster	*TIFF	USER FROM WEB INTERFACE	various	Internal
Drone Terrain Mapping dataset (includes RGB + Thermal imagery + telemetry)	rosbag file with images and gps information	.bag	INESCTEC	Drone	Internal
Santa Margarida Airfield	rosbag file with images and gps information	.bag	INESCTEC	Drone	Internal
São Jacinto Airfield	rosbag file with images and gps information	.bag	INESCTEC	Drone	Internal

Table 2 – WP2-3-4 update on new adopted datasets

4.3. WP 5

No new updates with respect to Issue n.1 of the present document have been implemented.

4.4. WP 6

No new updates with respect to Issue n.1 of the present document have been implemented.

5. FAIR Data

This section of the DMP presents the adopted measures to ensure that the data of the OVERWATCH project comply with the FAIR data principles of **Findability, Accessibility, Interoperability and Re-usability.**

The FAIR principles articulate the attributes data need to have to enable and enhance reuse, by humans and machines. It has long been recognized that it is not sufficient simply to post data and other research-related materials onto the web and hope that the motivation and skill of the potential user would be sufficient to enable reuse. There is a need for various things, including contextual and supporting information (metadata), to allow those data to be discovered, understood, and used.

According to the FAIR data principles, scientific data should be managed to be easily accessed and exchanged, promoting knowledge and innovation. In practice, the following general indications will be followed to assure the FAIR data principles:

Findability – clear naming of data and metadata, use of search keywords, and unique identifier that will optimize the potential of finding and re-using the data.

Accessibility – details on the repository in which the data will be made available and what tools are needed to access the data.

Interoperability – use of vocabularies, standards, formats or methodologies that will be used to enable data exchange, re-use and interoperability.

Re-usability – information on when and for which duration data are made available, and on licensing of data.

5.1 Making Data Findable

Data and research outputs findability have been ensured during the whole project lifetime by adopting a generally recognized naming convention for data and for metadata. Moreover, findability has been assured by two components:

1) a unique identifier (e.g. Digital Object Identifier - DOI) for data and metadata;

2) an easily accessible service to locate the data resource over time ensuring uniqueness in location.

Given such premises, the project fulfils the requirements to adopt an OpenAIR compliant repository such as Zenodo [RD01] ensuring to be compliant with all European directives. Zenodo is a free of charge, open data repository created by OpenAIRE and CERN and is financed by the EU.

5.2 Making Data Accessible

OVERWATCH supported the continuous effort to benefit for society by contributing to a global open science approach with the objective of transforming the scientific culture towards a more open, accessible, multidisciplinary, collaborative scientific community. OVERWATCH is fully compliant with

the open science policy of Horizon Europe as detailed in the Programme Regulation (Art. 14 and 39(3)) and further described in the General Model Grant Agreement (Art. 17 – Specific Rules).

To guarantee data accessibility, all public data and research outputs generated during the project lifetime, after proper referencing, have been published in the Zenodo open data repository. The adoption of Zenodo ensures to be compliant with all European directives devoted to guarantee the Open Access to research data outputs, i.e., ensuring accessibility to general public and interested entities (scientists, stakeholders, policy makers). The service offered by Zenodo can handle any file format of size up to 50GB, enabling the sharing of results and promoting data re-use. Using Zenodo increases the discoverability of the gathered data that are being made publicly available by OVERWATCH. Also, public documents (e.g. deliverables) have all as well made available on the OVERWATCH website by PC at M18, i.e. the end of the first reporting period (RP1) of the project, and after M42, i.e. the closure of all project activities, after formal approval by PO and reviewers. The documents are available in protected PDF files.

5.3 Making Data Interoperable

Interoperability and interconnection of generated data during the project lifecycle have been ensured through the adoption of conventional accepted formats and standards for all data generated within the OVERWATCH project. OVERWATCH adopted the Metadata Standards Directory [RD02] and FAIRsharing [RD03] as references to ensure that each product/component developed along project lifetime will meet traditional quality and consistency standards while they remain interoperable with other data sources at the same time. FAIRsharing standards also include standards for Metadata and guidelines for data management, providing guidelines for the most used geodata formats (e.g. Shapefiles, geoJSON, CSV, NetCDF, etc.), which also enables the creation and the provision of map layers through OGC standards (e.g. WMTS, WMS).

5.4 Making Data Re-Usable

Project research outputs such as software, algorithms, protocols, workflows and others, if deemed not key information for the project exploitation, are available for download and project outcomes review and validation enabling reusability.

OVERWATCH made its data publicly available under the Creative Commons Licensing scheme, which is also supported by Zenodo. Specifically, the Creative Commons Attribution-NonCommercial International 4.0, that: 1) enables the re-use of data, 2) ensures that the source and the authority of the data are recognized, and 3) protects the commercial interests of the participants, will be adopted as reference of the licensing scheme for making the data available.

6.Allocation of Resources

The Data Management Plan is a living document, and it has been updated by the lead beneficiary and reviewed by WP-leads and the Coordinator with the purpose of supporting the data management lifecycle for all data that have been collected, processed and/or generated by the project.

The Coordinator oversaw the updating of the DMP reporting changes and – together with the DM – was available to assist the consortium partners with specific questions in relation to the DMP.

The Coordinator is responsible for ensuring proper management and processing of all data in the project, complying with the EU data protection regulations. Moreover, the Coordinator oversees

uploading the deliverables to the Participant Portal and to place a copy on Microsoft SharePoint repository, adopted for the project, as agreed by the partners. The data shared among consortium partners, necessary for project implementation activities, are uploaded and stored in the adopted Microsoft SharePoint.

The public deliverables have been also uploaded by the Coordination team to the Zenodo Platform, including the public datasets related to the documents. Other types of public data must be also provided by partners to the Coordination team for uploading to Zenodo.

Data acquired by drones' acquisitions, a significant part of project output, were acquired inside military facilities, for this reason cannot be made publicly available due to security and regulatory restrictions.

Specifically, data collection activities were conducted within military facilities, and the resulting datasets are therefore subject to national security constraints. Any disclosure, sharing, or publication of these data requires prior authorization from the Army Chief of Staff, in accordance with applicable institutional and legal frameworks. As a result, the datasets are classified as restricted access data and cannot be openly shared or deposited in public repositories.

Generally, the responsibilities of the project members include:

- Update and classification of the data collected and generated in OVERWATCH
- Implementing and respecting the Data Management Plan.
- For those tasks that required processing of any kind of personal data, an analysis of the types of necessary personal data was made and it was responsibility of the leading partner for that specific Task/activity. Support from the DM and the Ethics Security Manager may be requested by the responsible partner if considered necessary.

Moreover, costs related to open-access to research data in Horizon Europe are eligible for reimbursement under the conditions defined in the Grant Agreement. Project beneficiaries are responsible for applying for reimbursement for costs related to making data accessible to others beyond the consortium.

The costs for making data FAIR includes:

- Fees associated with the publication of scientific articles containing project's research data in "Gold" Open access journals. The cost sharing, in case of multiple authors, shall be decided among the authors on a case-by-case basis.
- Data archiving at Zenodo and on other online data base: free of charge
- Copyright licensing with Creative Commons: free of charge
- OVERWATCH website operations: ad hoc budget was foreseen

Each partner is responsible for the data they produce. Any fee incurred for Open Access through scientific publication of the data is the responsibility of the data owner (authors) partner(s).

7. Data security

In compliance with the EU 2016/679, also known as General Data Protection Regulation (GDPR), Directive 2009/136/EC and in line with the OVERWATCH Grant Agreement art. 15.2, the OVERWATCH consortium always provided a safe and accessible environment for data storage, ensuring that data is preserved for future use. To this end, the internal SharePoint of the project Coordinator (ITHACA) has been adopted for the whole project duration and *ad-hoc* configured to be compliant with the GDPR. More detailed information ca be derived from the following internet page:

https://learn.microsoft.com/en-us/compliance/regulatory/gdpr. For this purpose, various measures have been implemented since the beginning of the project to ensure data security, and some additional actions added during project implementation to further strength security procedures. An update of such security measures is below provided:

1. Data encryption to prevent unauthorized access;
2. Restricted access control of sensitive data based on roles and responsibilities;
3. Backups of data and drafting of recovery plan in the event of a system failure or data breach;
4. Secure transfer protocols for sensitive data (e.g. SFTP);
5. Trusted repositories for long-term preservation and curation of data with established policies and procedures for data quality control, archiving, and access control by enforcing all partners to use MFA (Multi-Factor Authentication);
6. Well-organized folder structure and systematic file labelling to ensure final data set consistency. Project documents are classified through Microsoft Purview sensitivity labels according to dissemination level, confidentiality and personal data content.
7. A Record of Processing Activities (ROPA) has been internally established and maintained by the relevant consortium partners, in accordance with Article 30 of the GDPR, to document personal data processing activities related to project coordination, dissemination, workshops, demonstrations, and technical validation activities.
8. Privacy notices and information sheets have been provided where applicable for activities involving the collection or processing of personal data, including workshops, interviews, onsite demonstrations. WPs/Tasks Leaders responsible for such activities are, in the same way, responsible to appropriately inform participants in accordance with GDPR transparency obligations.

With specific regards to datasets acquired by drone flights, these were collected inside restricted military facilities, without the involvement of external participants, and do not contain personal data. Therefore, there is no risk of privacy breaches or personal data protection violations (e.g., GDPR).

In line with Horizon Europe requirements, the consortium, if requested, will:

- Provide metadata descriptions of the drone datasets where possible, without compromising sensitive information;
- Share aggregated, anonymized, or derived results when feasible and permitted;
- Ensure that any data sharing complies fully with security regulations and authorization procedures.

8. Ethics

OVERWATCH is fully aware that the project's activities may generate ethical, fundamental rights, privacy and data protection implications and is fully committed to adhere to the highest standards at the European and International level. All researchers in the project, at all levels (Principal Investigator, researchers, technicians, etc.), will commit to adhere to the European Code of Conduct for Research Integrity [RD06] and to uphold the highest ethical standards throughout the project, through forms circulated by the project coordinator.

Moreover, all project partners are obliged by European and national law (e.g., GDPR) to protect personal data. The OVERWATCH Coordinator ensured that the privacy and confidentiality of partner data is protected during data sharing and long-term retention. To this end, anonymized data and appropriate technical and organizational measures have been implemented to safeguard the data.

Additionally, the ethical and legal implications of data sharing have been carefully considered, ensuring that partners were properly recognized and accredited for their contributions, protecting against intellectual property rights infringements, and ensuring that data sharing was consistent with data protection and privacy laws.

All project partners acted in accordance with ethical guidelines and principles. No event of ethical violations happened during project lifetime.

Ethical issues related to DMP have been implemented in close synergy with Ethics deliverable of WP6, namely “D. 6.3 – Privacy, Ethics and security report” due on M12, and then updated at M42.

References

ID	Title	Access Date
[RD01]	Zenodo OpenData Repository. Link.	2023
[RD02]	RDA Metadata Standards Directory .Link.	2023
[RD03]	FAIRsharing.org Standards, databases, policies. Link	2023
[RD04]	OVERWATCH Grant agreement No. 101082320	2023
[RD05]	OVERWATCH Consortium Agreement	2023
[RD06]	European Code of Conduct for Research Integrity	2023
[RD07]	Data Management Plan	2026