Horizon Europe Framework Programme (HORIZON)

Call: HORIZON-WIDERA-2023-ACCESS-02

Project type: Coordination and Support Action

Topic: HORIZON-WIDERA-2023-ACCESS-02-01 - Twinning Bottom-Up

Grant Agreement Number: 101160022

Project Name: **Verification and Analysis for Safety and Security of Applications in Life**

Project Acronym: **VASSAL**

D1.3 First version of the Data Management Plan

Document identification			
Status	Final	**Due Date**	30. 11. 2024
Version	1.0	**Submission date**	30. 11. 2024
Dissemination level	PU – Public	**Deliverable ID and Title:**	D1.3 First version of the Data Management Plan

This project is funded under Horizon Europe Framework, Grant Agreement no 101160022

Funded by
the European Union

Related WP	WP1	**Document reference**	D1.3
Lead participant	BUT	**Lead Author**	Bohuslav Křena (BUT)
Contributors	Milan Češka (BUT) Martin Jírovec (BUT) Sára Veselá (BUT)	**Reviewers**	Florian Zuleger (TUW) Julien Signoles (CEA)

Keywords
Data Management Plan (DMP), software, analysis, verification, tools, FAIR data, GDPR, accessibility, interoperability, reusability, open access, open source, copyleft licenses

Disclaimer

Funded by the European Union under Horizon Europe programme, Grant Agreement no 101160022. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Horizon Europe programme. Neither the European Union nor the granting authority can be held responsible for them.

History of changes

Revision history			
Version	Date	Created/Modified by	Comments
0.0	02.08.2024	Sára Veselá (BUT)	Creating the document
0.1	18.10.2024	Bohuslav Křena (BUT)	First draft of the plan
0.2	8.11.2024	Bohuslav Křena (BUT)	Revision based on the comments by Martin Jírovec (BUT) and Milan Češka (BUT)
0.3	20.11.2024	Bohuslav Křena (BUT)	Version ready for the review by Florian Zuleger (TUW) and Julien Signoles (CEA)
0.4	27.11.2024	Martin Jírovec (BUT) Bohuslav Křena (BUT)	Version ready for final check by project coordinator
1.0	29.11.2024	Milan Češka (BUT)	Final version

Executive summary

This document introduces the first version of the Data Management Plan (DMP) for the VASSAL project. It provides an overview of the research data used within the VASSAL project. As the research performed within the VASSAL project concentrates mainly on the improvement of *automated methods for ensuring safety and security of software* and associated analysis and verification tools, the most data has a special character, i.e., analysis and verification tools with examples showing the purpose and the performance of the tools. After data summary, typical means for sharing the tools and with them associated data and for publishing the achieved results are elaborated to assure that the project is compliant with FAIR data principles. Allocation of resources to ensure FAIR data implementation, data security, and ethical issues are then discussed. DMP is considered as a life document. It will be provided with an updated version at M18 and at M36.

List of Abbreviations

Abbreviation	Description
BUT	Brno University of Technology
TUW	Technical University of Vienna
CEA	The French Alternative Energies and Atomic Energy Commission
PSU	The Pennsylvania State University
HISRO	Honeywell International
EC	European Commission
HE	Horizon Europe

Contents

1. INTRODUCTION.......... 5
1.1 THE VASSAL PROJECT.......... 5
1.2 PURPOSE OF DELIVERABLE.......... 5
1.3 INTENDED AUDIENCE.......... 5
2. DATA SUMMARY.......... 5
3. FAIR DATA.......... 8
3.1 MAKING DATA FINDABLE AND ACCESSIBLE.......... 8
3.2 MAKING DATA INTEROPERABLE.......... 10
3.3 INCREASING DATA REUSABILITY.......... 10
4. ALLOCATION RESOURCES.......... 11
4.1 COSTS.......... 11
4.2 PERSONNELS AND RESPONSIBILITIES.......... 11
4.3 ARCHIVING AND LONG-TERM ACCESSIBILITY.......... 11
5. DATA SECURITY.......... 12
6. ETHICS.......... 12
7. CONCLUSION.......... 13

1. INTRODUCTION

This document outlines the plans and procedures essential for the successful implementation of the project. It serves as a comprehensive guide to ensure the delivery of high-quality outputs, effective risk management, and active collaboration among consortium members.

1.1 THE VASSAL PROJECT

The objective of the VASSAL project is to elevate the research profile, visibility and reputation of Brno University of Technology (BUT) by fostering excellence in research and innovation (R&I) as well as by leveraging the institutional R&I governance and administration competencies while ensuring the integration and sustainability of the project. This will be achieved through intensive collaboration and knowledge sharing with internationally renowned consortium partners Vienna University of Technology (TUW), CEA, Penn State University (PSU) and Honeywell International (HISRO). The VASSAL project will use a series of twinning actions focused on several key areas to elevate the excellence of capacities and research profile of all consortium partners, mainly BUT. VASSAL aims to raise the reputation of participating institutions and deepen their collaboration while establishing new partnerships with stakeholders and opening funding opportunities.

The VASSAL project is dedicated to seeking significant advancements in its scientific domain of software safety and security and delivering cutting-edge technologies by integrating model-based design (MBD) preconditions with formal methods (FMs) for automated analysis and verification. This combined approach ensures software reliability from development through to operations. By assessing the economic implications of deploying these advanced verification tools, VASSAL aims to provide insights into the benefits and challenges for end-users, particularly in critical applications such as automotive and aerospace systems.

VASSAL is coordinated by the Brno University of Technology (BUT), with the participation of a total of four partners from EU countries and the USA.

BRNO UNIVERSITY OF TECHNOLOGY TU WIEN TECHNISCHE UNIVERSITÄT WIEN cea PennState Honeywell

1.2 PURPOSE OF DELIVERABLE

Data Management Plan (DMP) outlines the data life cycle and sets guidelines on data collecting, processing, generating, storage, handling, maintenance, sharing, methodology and standards, terms of open access, data security, as well as curation and preservation. We stress here the importance of the availability of the research data (in the VASSAL project, mainly analysis and verification tools with examples that demonstrate their abilities and performance) to other researchers to have a chance to verify our conclusions and increase uptake of our results by industry. We also discuss data security and ethical issues connected with the project.

1.3 INTENDED AUDIENCE

The primary audience for the Data Management Plan (DMP) includes the VASSAL consortium to have at one place comprehensive information about data management and the European Commission to check that the consortium deals with data management correctly.

2. DATA SUMMARY

Data Management Plan (DMP), updated as needed, will follow the FAIR principles and outline the data life cycle and set guidelines on data collecting, processing, generating, storage, handling, maintenance, sharing, methodology and standards, terms of open access, data security, ethics, as well as curation and preservation.

The most of the research performed within this project aims at improving *automated methods for ensuring safety and security of software*. The original analysis and verification tools like Predator[1], ANaConDA[2], z3-noodler[3], and Perun[4] are provided with a rich set of examples to show the purpose of the tools as well as to demonstrate their performance. Such examples, sometimes called case studies or even benchmarks, can be seen from DMP point of view as a special kind of datasets despite in the terminology used within officially provided template[5], they are mentioned as *"other research outputs"*. We, however, handle them in this document in the same way as common data whenever it is meaningful and describe how they will be managed and made available for re-use, in line with the FAIR principles.

The already created examples will be naturally re-used for tools improved within the VASSAL project to evaluate their new abilities and performance. As the tools perform software analysis and verification, their inputs are mainly source codes of programs that are indeed text files (following the rules of a particular programming language). In some cases, models of the system under consideration in different formal languages, executable software, properties specification that the system should fulfil can be taken as an input of the tool as well.

The output of such tools can be a simple text or structured data depending on the concrete research tool and analysis performed. As the output of the tools is often intended for humans (more precisely, for software developers), the size of the generated data is usually quite small (order of kB). When the data generated by the research tool are intended for postprocessing and showing the results using, for instance, graphs, it can be bigger but typically not bigger than the order of MB. Thus, the size of the input and output data does not require any special attention.

In the following table we list common types of files used within our tools.

[1] https://www.fit.vut.cz/research/group/verifit/public/tools/predator/

[2] https://www.fit.vut.cz/research/group/verifit/public/tools/anaconda/

[3] https://github.com/VeriFIT/z3-noodler

[4] https://github.com/Perfexionists/perun

[5] https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/temp-form/report/data-management-plan_he_en.docx

Table 1: Typical file types used within VASSAL project tools

Category	File Types	Description
Readme	Text/MD[6] (MD – Markdown)	Basic description of a tool with instruction how to install and use it
Licence	Text	License for a tool specifying the rights granted to users
Documentation	Text/MD/PDF/ doc/docx/rtf/ HTML	Documentation of a tool (e.g., installation process, typical usage, the foundations on which it stands, provided examples, etc.)
Makefile	Text (make)	Command-line interface for building a tool
Scripts	sh/pl/py/php/ bat	Scripts describing tasks execution
Source Codes	c/h/cc/cpp/hh/ java	Implementation of a tool functionality or inputs for the tool (e.i., snippets of code for the analysis or verification)
Configuration	json/cvs/yml/xml	Structured data for setting up a tool parameters
Log Files	Text	Describe results of a tool execution and eventual errors
Output Data	json/cvs/yml/xml	Structured data produced by a tool as outcome of the analysis
Figures	svg/png/gif/PDF	Images used for user interface or produced by a tool (outputs)

Apart from the research data described above, we need to collect contact information such as names, phone numbers, and email addresses of project partner representatives, as well as external individuals and stakeholders, including their affiliations, to manage the project. All this data will be handled with care and in compliance with GDPR and partner's internal rules.

Finding right case studies to demonstrate tool abilities is usually a quite hard task. One can create own examples (they are usually quite simple but the least trustworthy), re-use examples from similar tools (it is great for tools comparison), select suitable examples from publicly available benchmark (in our area, Competition on Software Verification SV-COMP[7] plays a prominent role) or extract parts of the real-life software (it is the most trustworthy but the most hard-working approach even if somebody from industry is willing to provide their software to university for analysis). We strive for providing our tools with comprehensive and carefully documented (it can be seen as a kind of metadata) examples. Thus, we intend also to make examples used within this project publicly available to allow other researchers to check our results and to compare their tools with ours.

[6] https://www.markdownguide.org/getting-started/

[7] https://sv-comp.sosy-lab.org/

3. FAIR DATA

The VASSAL project is committed to ensuring that its tools and the associated data are both findable and accessible. This is achieved through the use of trusted repositories and mechanisms that guarantee long-term availability. Providing complete data (primarily in the form of software artifacts) is a cornerstone of our strategy to enhance research transparency and credibility. By enabling other researchers to reproduce our results, we aim to foster trust and reliability within the scientific community.

Open Source and Reusability
In line with our commitment to openness, VASSAL will make its tools publicly available as open-source resources. This approach not only benefits the academic community by facilitating further research and experimentation but also serves industrial stakeholders. Businesses will have the opportunity to test our tools and validate their efficacy before adopting them in their operations, thus bridging the gap between research and practical application.

Maximizing Accessibility While Respecting Restrictions
While VASSAL is dedicated to maximizing access to and re-use of its tools and examples, certain data may be protected due to confidentiality, intellectual property, or other constraints. In such cases, access will be restricted, but the project will ensure that the majority of its research outputs remain openly available. Through this balanced approach, VASSAL aspires to advance open science principles while maintaining respect for necessary protections, ultimately contributing to both academic progress and industrial innovation.

3.1 MAKING DATA FINDABLE AND ACCESSIBLE

VASSAL adopts a multi-layered strategy to ensure data accessibility:

1. **Public Dissemination**: Open data will be shared through public channels, including the project's website and trusted repositories such as Zenodo and arXiv, ensuring wide reach and easy access.
2. **Internal Data Management System**: An internal repository will serve as the primary tool for collecting, processing, sharing, and managing research data within the consortium. This system will consolidate information on software verification, analysis, synthesis, performance, and related economic considerations, as well as other data and materials produced during the project. It will include relationships between tools, examples, and characterizations conducted during the research. This repository will ensure transparency, enable traceability, and support collaboration among partners.
3. **Repository Integration**: Our tools and examples will be made publicly accessible through the university website, GitHub, Zenodo, and arXiv repositories, leveraging its robust features for data sharing and compliance with FAIR principles.

By combining public and internal mechanisms, VASSAL ensures both broad dissemination of research outputs and efficient internal data handling, supporting the project's commitment to open science while maintaining operational efficiency and traceability. The VASSAL project ensures robust and multi-faceted data accessibility by leveraging a variety of platforms and tools to serve both public and internal audiences.

Platforms

The VASSAL project uses the following platforms:

1. **VASSAL Website**
   The public section of the VASSAL website (https://vassal.fit.vut.cz/) serves as a primary dissemination tool. It hosts all publicly accessible deliverables, peer-reviewed scientific articles, newsletters, and related publications, ensuring third-party access throughout the project duration.

2. **Public Repositories**
   To comply with Horizon Europe Open Access requirements and amplify the project's impact, research data will be deposited in widely recognized public repositories, including:

- **Zenodo**: for long-term storage of open data and research outputs, complete with persistent identifiers for easy access.
- **GitHub**: for sharing source code and software-related artifacts.
- **OpenAIRE**: for connecting research materials to the European Commission Funded Research Community.

3. **VASSAL Internal Google Drive**
   An internal repository will be maintained via Google Drive for secure document storage and sharing. This platform will be accessible to all project beneficiaries throughout the project's duration, enabling them to upload and download all documents, including restricted ones.

4. **EC Participant's Portal**
   Deliverables (both public and confidential), project reports, or other documents are made available to project partners and the European Commission via the SYGMA Portal. The final summary report will also be accessible through the EC Cordis platform (https://cordis.europa.eu/).

Metadata

VASSAL ensures that all published data is accompanied by comprehensive metadata to enhance discoverability, usability, and compliance with open science standards. Alongside the project name and Grant Agreement (GA) number, the metadata will include the following key features:

- **Abstract/Description**: A concise summary providing an overview of the data's content and purpose.
- **Access and Licensing Information**: Clear details on usage rights and access conditions.
- **Associated Project and Community**: Links to the VASSAL project and relevant scientific communities.
- **Associated Publications and Reports**: Connections to related documents and research outputs.
- **Bibliographic Information**: Proper citation details for academic referencing.
- **Digital Object Identifiers (DOIs)**: Persistent identifiers to ensure data are uniquely identifiable and accessible.
- **Grant Information**: Reference to funding support and acknowledgment of the European Commission.
- **Keywords**: Carefully curated terms for enhancing searchability and thematic categorization.
- **Language**: Information on the language(s) used within the data.
- **Version Numbers**: Sequential identifiers for tracking data updates.

Keywords

Specific keywords will be assigned to all public data to aid searchability. The consortium will also develop a general set of keywords applicable across data, publications, and deliverables to maintain consistency and relevance.

Versioning

Versioning is a critical component of VASSAL's data management strategy. As an example, all data hosted on Zenodo will feature DOI versioning, provided by Zenodo's native DOI service. This ensures that users can track updates and access specific iterations of data, enhancing transparency and reliability in research dissemination.

Tools and artifacts current publication practices

Our tools are typically published either on the university web, using GitHub[8] or on the web site of the tool when we provide some tool extension or plug-in only. The tools are provided together with case studies and their description (a kind of metadata that, of course, differ for particular tools).

[8] https://github.com/

When publishing some particular research results achieved within the tool development, articles and papers are identified using Digital Object Identifier - DOI[9]. To attach software artifacts to the paper, the article or the report, we store them to arXiv[10] or Zenodo[11].

We consider these instruments as standard for the particular purposes and we see them as trusted. Of course, there is a risk that university web structure can be reorganized due to marketing reasons, however, it does not happen too often to the extent that it affects the tool page URL.

Our tools and with them associated data are intended to be openly available. The only possible exception is when we cooperate with industry on analysis and verification of their code. In such cases, we are not usually allowed to publish such code and a special attention is needed when publishing the results at conferences or in journals because companies do not like to show that some bugs have been found in their software products. We have no evidence of such a case in this project yet, however, if it happens we will report it in the later version of this deliverable.

The tools and associated data are accessible via standardized protocol HTTPS and we do not plan to identify persons accessing the tools and the data. We expect that if somebody publishes an article, paper or tool using our results, (s)he acknowledges it. Based on the character of the research data (meaning tools and their examples) we provide, we do not consider approval of access and collecting personal identifications as meaningful.

3.2 MAKING DATA INTEROPERABLE

Each analysis and verification tool has a different purpose and thus, different inputs and outputs. When reasonable, we can employ our tool developed within previous projects - UNIversal analysis adapTEr (Unite)[12] that is based on the Open Services for Lifecycle Collaboration (OSLC)[13] standard to implement interoperability between analysis, verification and similar tools. Unite provides an easy way of adding an OSLC Automation interface to analysis and verification tools by leveraging their command-line similarities. The adapter consists of two main components: Analysis Adapter and Compilation Adapter. The Compilation Adapter manages SUT resources, and the Analysis Adapter executes analysis on SUT resources using any configured analysis tool. Unite is supplemented with an Eclipse Jetty web server[14] that supports many common communications protocols and offers integrations with many other technologies and with a SPARQL server Apache Jena Fuseki[15] for user's convenience (to make the setup process easier) which allows the adapter to be connected to a SPARQL[16] triplestore for resource persistence and query capabilities.

3.3 INCREASING DATA REUSABILITY

Upon the completion of the VASSAL project, ownership of tools and data will reside with its original owners. To encourage the widest possible re-use of tools and data, the project will use copyleft licences like GNU General Public License, MIT License, or Creative Commons licenses. These licenses will allow for the re-use, distribution, and modification of the data, while ensuring proper attribution to the original creators. In cases where a more restrictive

[9] https://www.doi.org/

[10] https://arxiv.org/

[11] https://zenodo.org/

[12] https://pajda.fit.vutbr.cz/verifit/unite

[13] https://open-services.net/

[14] https://jetty.org/index.html

[15] https://jena.apache.org/documentation/fuseki2/index.html

[16] https://www.w3.org/TR/sparql11-query/

license is necessary, the project will carefully evaluate and justify the reasons for such a decision. Additionally, all open data will include a disclaimer of liability regarding its re-use, further promoting transparency and responsibility.

While there is no defined time limit for the access or re-use of the data, the project will deposit all artifacts in reputable repositories that ensure data integrity at the bit level. This will guarantee the preservation of data accuracy over time. However, at this stage, there are no plans for an ongoing data curation policy to ensure full long-term digital preservation beyond the project's closure.

In certain cases, the project consortium may decide to impose an embargo on specific data, primarily in connection with potential patent applications arising from the project's results. The justification for such embargoes will be thoroughly evaluated and agreed upon by the consortium.

4. ALLOCATION RESOURCES

In this section, we discuss resources needed to implement FAIR data principles.

4.1 COSTS

No direct costs are expected for the management of FAIR data as existing infrastructure will be used. Costs connected with operations and maintenance of ICT owned by the project partners will be covered by indirect costs of the project. At universities, the cost of core ICT is usually covered centrally by the university budget. Costs of ICT facilities that are not provided by the university but operated by a faculty are covered by the faculty budget. Only specialized ICT required by special needs of some project is funded directly by the project budget. We, however, do not consider such circumstances in this project.

4.2 PERSONNELS AND RESPONSIBILITIES

The data management in the VASSAL project will be the responsibility of each research area leader, namely:

- RA1 - Logics and Automata: Ondřej Lengál (BUT),
- RA2 - Model-based Design, Analysis, and Synthesis: Ezio Bartocci (TUW),
- RA3 - Verification and analysis on the source code level: Florian Zuleger (TUW),
- RA4: Economic implications: Radek Doskočil (BUT).

They will be led and supported by the leader of WP3 Joint research - Tomáš Vojnar (BUT).

4.3 ARCHIVING AND LONG-TERM ACCESSIBILITY

Published and FAIR-compliant data will be archived in widely recognized open data repositories. This approach underscores the project's commitment to open science, enhancing the global research community's ability to build upon VASSAL's findings. VASSAL plans to use trusted repositories, such as Zenodo, to ensure long-term accessibility and reusability of the data. We consider the assured lifetime of at least 20 years of Zenodo servers as more than sufficient. Unfortunately, quick development of operating systems, programming languages, frameworks, and libraries goes hand-in-hand with compatibility issues that make software analysis and verification tools obsolete much sooner. Thus, we consider it acceptable in appropriate cases to use the institution's websites, arXiv or even GitHub. Universities are the most stable institutions, thus, their websites (arXiv operated by the Cornell University) seem as stable enough. The only questionable from this point of view is GitHub as it is owned by Microsoft that can change the policies and conditions quite quickly, however, it is widely used and provides many comfortable services.

5. DATA SECURITY

At the outset of the VASSAL project, the research consortium will establish and agree on the roles, responsibilities, and rights concerning data collection, data management, and data usage. This includes a clear delineation of who is authorized to access, use, and manage the research data throughout the project's lifecycle, ensuring all rules regarding the safety and security of data set by the individual institutions involved are respected. The project is not expected to work with sensitive data, and therefore, all data management activities will be carried out in compliance with the safety standards of the participating institutions.

Throughout the project, research data will be accessible only to consortium members who have been specifically accredited and whose data usage has been approved by the Principal Investigator or another authorized project consortium member. Each partner will be responsible for the curation, preservation, dissemination, and appropriate deletion of data in their possession. The retention period for curated data will align with the retention policies for other project results and will be determined collectively by the project consortium partners.

All data collected or acquired during the project will be stored in a secure IT environment, either on the premises of project consortium partners or in a secure cloud environment provided by approved IT service providers. For instance, internal project data, such as deliverables, meeting minutes, and work package data, will be stored on Google Drive, which is provided to BUT based on a bilateral agreement between BUT and Google. Research data can also be stored on personal computers of the researchers or on research servers operated and maintained by the respective institutions. This setup is considered reasonable from a security perspective, taking into account the non-sensitive nature of the data being handled.

Access to this data will require registration and authentication, ensuring that only authorized personnel can access the data. The Principal Investigator will review and approve any applications for data use, ensuring compliance with the project's data management policies. For data access, secured communication channels will be employed to protect the integrity and confidentiality of the research data.

To ensure long-term and secure preservation of published research data, the project will use certified, OpenAIRE-compliant repositories. Public data will be stored in trusted repositories, as discussed above, guaranteeing that it remains accessible, reusable, and preserved according to best practices. This approach will ensure the data’s security and integrity throughout the project and beyond.

6. ETHICS

The VASSAL project is committed to ensuring the highest standards of privacy, data protection, and ethical practices throughout its lifecycle. In line with the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679), the project will take appropriate measures to secure the privacy of data subjects. The project consortium has implemented both technical and organizational safeguards to protect personal data throughout the project's duration. All processes that involve personal data are designed with GDPR principles in mind. These processes incorporate privacy by design, ensuring that the highest possible privacy settings are applied by default.

The Principal Investigator, along with the project’s data processors, will retain clear, unambiguous, and individualized confirmation of consent from data subjects. Data subjects will retain the right to withdraw their consent at any time, as required by the GDPR. During and after the project, the project coordinator will ensure transparency by publicly disclosing which data have been collected, the lawful basis for their processing, the specific purposes for which they were collected, and the duration of their retention. If data is shared with third parties or outside the European Economic Area (EEA), this will also be clearly stated.

Importantly, the data used in this project does not contain any sensitive information, such as medical or genetic data, and no critical experiments (e.g., those involving humans, embryos, or other vulnerable populations) are planned. Therefore, the project does not require ethical review of this nature. However, some attention will be necessary for research activities in RA4 - Economic Implications, as companies involved in the project are often cautious about sharing internal financial data. While this is not classified as an ethical issue, the project's Ethics and Inclusiveness Committee (EIC, defined in D1.1, Section 3.9) will be engaged to ensure that research complies with best practices. Moreover, all research results will need to be approved by the involved project partners prior to publication.

In addition to the rights of data subjects, such as the right to request a portable copy of their data in a commonly used format and the right to have their data erased under specified conditions, the project will ensure that these rights are upheld throughout the duration of the project and beyond its closure. The project coordinator will provide clarity on the data sharing practices, including the duration of data retention and any external parties involved in data handling.

The GDPR compliance will be managed by an officer at BUT, who will oversee and ensure adherence to data protection standards and practices throughout the project. Ethical considerations concerning data collection and use are comprehensively addressed in the ethics self-assessment section of the grant application, outlining the project's commitment to research integrity and responsible data management.

7. CONCLUSION

This is the initial version of the Data Management Plan. It is not supposed to stay as it is, however, it will be rather a living document that responds to issues connected with data management when they arise. Updated version of the Data Management Plan (DMP) will be reported as Deliverable D1.4 at M18 and Final version of the Data Management Plan (DMP) will be reported as Deliverable D1.5 at M36.