

HORIZON-WIDERA-2023-ACCESS-03

BIOECONOMY EXCELLENCE ALLIANCE FOR STIMULATING
INNOVATIVE AND INCLUSIVE GREEN TRANSITION

BEAMING

D1.3 – Data Management Plan

Lead Contractor: BME

Author(s): Balázs Imre, Anikó Fehér

Date: 26/07/2024

This document corresponds to D1.3 of the BEAMING project (contract no. 101137131) and, in particular, to Work Package 1 (M1-16) led by the Budapest University of Technology and Economics (BME).

This document contains all relevant information regarding data management.

Project details			
Project acronym	BEAMING	Start/ Duration	01/01/2024 48 months
Topic	HORIZON-WIDERA-2023- ACCESS-03-01	Call identifier	HORIZON-WIDERA- 2023-ACCESS-03
Type of Action	HORIZON Coordination and Support Actions	Coordinator	BME
Contact persons	Balázs Imre (imre.balazs@edu.bme.hu) Anikó Fehér (feher.aniko@vbk.bme.hu) Boglárka Tóth (toth.boglarka@bme.hu)		
Website	https://beamingproject.eu/		

Deliverable details			
Number	D1.3		
Title	Data Management Plan		
Work Package	WPI		
Dissemination level	Public	Nature	Document, report
Due date (M)	6	Submission date (M)	7
Deliverable responsible	1. BME	Contact person	Balázs Imre

Deliverable Contributors				
	Name	Org.	Role / Title	E-mail
Deliverable leader	Balázs Imre	BME	Coordinator	imre.balazs@edu.bme.hu
Contributing Author(s)	Anikó Fehér	BME	Contributor	feher.aniko@vbk.bme.hu
Reviewer(s)	Boglárka Tóth	BME	Reviewer	toth.boglarka@bme.hu
	Liliya Pullman	FhG- ISI	Reviewer	Liliya.Pullmann@isi.fraunhofer.de
	Eleftheria Moraiti	CluBE	Reviewer	e.moraiti@clube.gr
Final review and quality approval	Liliya Pullman	FhG- ISI	Reviewer	Liliya.Pullmann@isi.fraunhofer.de
	Boglárka Tóth	BME	Reviewer	toth.boglarka@bme.hu
	Balázs Imre	BME	Reviewer	imre.balazs@edu.bme.hu

Document History			
Date	Version	Name	Changes
06/18/2024	V0.1	First draft	
07/17/2024	V0.2	Updated draft	Modified based on internal review
07/23/2024	V1.0	Reviewed deliverable	Modified based on partners' comments
07/26/2024	V1.1	final version	Minor changes implemented during the final review

Executive Summary

The Data Management Plan (DMP) for the BEAMING project is a comprehensive document designed to ensure the efficient, secure, and compliant handling of all data generated and used throughout the project lifecycle. This plan outlines the key strategies, procedures, and responsibilities associated with data management, providing a clear roadmap for data collection, storage, sharing, and preservation.

Key components of the DMP include detailed descriptions of the types and formats of data that will be generated, the methods and tools for data collection and validation, and the security measures in place to protect the data. The DMP also addresses data-sharing policies, ensuring that data is accessible to authorized users while maintaining necessary restrictions and confidentiality.

In addition to outlining the roles and responsibilities for data management, the DMP provides guidelines for long-term data preservation and archiving, ensuring that data remains accessible and reusable beyond the project's duration. Quality assurance procedures are included to maintain data accuracy and consistency, and the plan ensures compliance with ethical guidelines and legal requirements.

By reading this DMP, all project participants will understand their roles and responsibilities in managing the project data, the protocols they must follow, and the measures to address potential risks. This ensures a coordinated approach to data management, contributing to the project's overall success and advancing knowledge in our field.

Acronyms and Abbreviations

ACRONYMS	EXPLANATION
CEE	Central-Eastern European
CA	Consortium Agreement
DMP	Data Management Plan
DMP	Data Management Plan
DPO	Data Protection Offices
DOI	Digital Object Identifier
EC	European Commission
EOSC	European Open Science Cloud
ERA	European Research Area
EU	European Union
FAIR	Fairness, Accessibility, Interoperability, and Reusability of data
GDPR	General Data Protection Regulation
GA	Grant Agreement
NDA	Non-Disclosure Agreement
QH	Quadrupole Helix
R&I	Research and Innovation
SEE	South-Eastern European
WP	Work Package

TABLE OF CONTENTS

1.	Introduction and Overview of BEAMING project.....	7
1.1	BEAMING Project	7
1.2	Why read a Data Management Plan?	8
2.	Data Summary	8
2.1	Purpose of the Data Collection.....	8
2.2	Data Structure, Metadata, and Documentation.....	9
2.3	Method and Tool of the Data Collection	10
3.	Making Data FAIR.....	11
3.1	Making Data Findable, Including Provisions for Metadata.....	12
3.2	Making Data Accessible	13
3.3	Making Data Interoperable	14
3.4	Increase Data Re-use	14
4.	Ethical and Legal Compliance.....	15
4.1	Intellectual Property Rights.....	15
4.2	General Data Protection Regulation	16
	Anonymisation and Pseudo-anonymisation of Personal Data	17
5.	Data security	18
5.1	Data Protection Officer	18
6.	Conclusion.....	19

1. Introduction and Overview of BEAMING project

1.1 BEAMING Project

BEAMING, an ambitious initiative, sets its sights on fostering excellence in innovation and knowledge valorisation within the bioeconomy domain. The project hinges on collaborative efforts among higher education institutions, emphasizing Central-Eastern and South-Eastern European (CEE and SEE) EU Member States and the Western Balkans. The overarching goal is to bolster the global competitiveness and visibility of higher education institutions (HEIs) by facilitating effective technology and know-how transfer between Widening countries and more developed bioeconomies and research & innovation (R&I) ecosystems.

Central to BEAMING's mission are seven specific objectives aimed at catalysing transformative change. These include capacity-building initiatives for early-career researchers, reforming institutional practices and policies, fostering networking and cross-disciplinary collaboration through sustainable Communities of Practice, and designing joint research and innovation strategies. Moreover, the project strongly emphasizes embracing Open Science practices, strengthening tech transfer capabilities, and promoting inclusive institutional cultures, particularly regarding gender equality.

BEAMING adopts the Quadruple Helix innovation ecosystem approach, advocating for collaborative frameworks where higher education institutions work hand in hand with industry, government, and civil society. This approach aims to amplify innovation capacity and enhance the real-world applicability of research outcomes. The project is committed to developing local and regional implementation strategies and roadmaps, aligning closely with the European Research Area (ERA) Policy Agenda, focusing on advancing the bioeconomy and

circular economy domains within higher education. BEAMING strives to drive meaningful and sustainable change in the bioeconomy landscape through these concerted efforts, propelling higher education institutions toward outstanding excellence and impact.

1.2 Why read a Data Management Plan?

Reading the Data Management Plan (DMP) is crucial for all partners involved in the BEAMING project. The current document is the first draft of BEAMING DMP (D1.3). It will be updated twice (D2.2 and D2.3) during the project's lifetime. In this first draft, we will introduce partners to data management proceedings.

The DMP provides comprehensive guidelines on collecting, storing, sharing, and protecting data throughout the project. By understanding and adhering to these protocols, partners can ensure that data management practices are consistent and compliant with ethical and legal standards.

2. Data Summary

This section provides a comprehensive overview of the data generated and utilized throughout the project. It details the types of data collected, including their formats and sources, and outlines the methodologies employed in data collection and processing. Additionally, this summary highlights the key characteristics and volumes of the data, ensuring transparency and clarity in how data is managed. Description of the types and formats of data generated during the project.

All produced data during the BEAMING project are summarized in the Data Summary table. More details are provided in Section 2.2.

2.1 Purpose of the Data Collection

The primary purpose of data collection in the BEAMING project is to advance innovation and valorisation of knowledge generated at HEIs within the bioeconomy domain. By systematically gathering relevant data, BEAMING aims to generate insights that drive the development of

Funded by the European Union under grant agreement N° 101137131. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the Research Executive Agency (REA). Neither the European Union nor the granting authority can be held responsible for them.

sustainable and competitive bio-based value chains across CEE and SEE EU Member States and the Western Balkans. This data will support informed decision-making, enable rigorous analysis, and facilitate the evaluation of project outcomes.

Additionally, collecting data from partners will help identify gaps, trends, needs and opportunities within the bioeconomy sector, fostering a more integrated approach to research and innovation. Ultimately, the collected data will underpin efforts to enhance the global competitiveness of higher education institutions in Widening countries, promote effective technology and know-how transfer, and support collaboration across the European Union.

2.2 Data Structure, Metadata, and Documentation

The data structure is designed to ensure that all collected data is organized systematically, facilitating easy access, analysis, and integration. Each dataset is categorized according to specific criteria, such as type, source, and relevance to the respective work packages (WPs), ensuring consistency and clarity. The naming procedure is described in the section on Dataset Naming.

Metadata is crucial in providing detailed descriptions of the data, including information on its origin, format, and any processing transformations it undergoes during the project. This metadata ensures that all data is contextually understood and can be accurately interpreted and re-used by project participants and stakeholders.

Thorough documentation accompanies both the data and metadata, outlining the procedures for data collection, processing, and storage. This documentation serves as a guide for all project partners, ensuring uniformity in data handling and promoting adherence to best practices. It includes guidelines for data entry, templates for metadata, and instructions for using the SharePoint platform for data management.

The Data Summary Table, to be filled out by partners, will further standardize data collection.

The **Data Summary Table** contains the following:

- Related WP
- Related task
- Title
- Keywords: add 2-3 words describing the data to facilitate the search
- Purpose of the data collection: concerning the project objectives
- Collector: name and institution
- Source of Data: such as surveys, reports, collection of action plans, contact lists, videos, software, etc.
- Data type: text, image, numerical, etc.
- Data format: such as .dox, .xls, jpeg, etc.
- Size (KB/MB/GB/TB)
- Does it include personal data? YES / NO
- Does it include other sensitive data? YES / NO
- Reusability for further research or projects? YES/NO
- Target user: consortium, researchers, policymakers, citizens, etc.
- Data storage location: SharePoint, repository, project website, Zenodo, etc.
- DOI (if it has)
- Data sharing rules: public, consortium, etc.
- Any additional comment (like if it is not open data, please explain.)

The information listed above will be collected from partners and included in the updated DMP.

The Data Summary table can be found on Sharepoint: [BEAMING - Data Summary.xlsx](#)

2.3 Method and Tool of the Data Collection

In the BEAMING project, data collection is systematically organized and managed using **SharePoint**. This platform is the central repository where all data is uploaded and stored, structured according to work packages (WPs). By SharePoint, we ensure that data is securely stored,

easily accessible, and efficiently managed across all project partners. This ensures that all project data is accessible to the partners, facilitating collaboration and transparency. Access to the SharePoint repository is restricted to authorized personnel, ensuring that the data is secure and available only to those with the appropriate access. Each work package has a dedicated section on SharePoint, allowing team members to seamlessly upload, share, and collaborate on data. This method not only enhances data organization and retrieval, but also fosters real-time collaboration.

[BEAMING SharePoint](#)

3. Making Data FAIR

In the context of Horizon Europe, Findable, Accessible, Interoperable, and Re-usable (FAIR) principles refer to data management and sharing guidelines that emphasize Fairness, Accessibility, Interoperability, and Reusability of data. These principles are intended to facilitate data exchange and maximize its value and utility while ensuring privacy and security. The European Commission (EC) has strongly advocated adopting these principles across various sectors, including research, science, and industry.

The FAIR principles are essential for advancing data-driven research, innovation, and collaboration within the European Union and beyond. By following these principles, organizations and institutions can improve the discoverability, accessibility, and usefulness of their data, thereby driving scientific progress, economic growth, and societal benefits. The EU actively promotes these principles to foster a culture of data sharing and collaboration among research communities, industry sectors, and government agencies.

3.1 Making Data Findable, Including Provisions for Metadata

To improve the accessibility of a dataset, it must be quickly and easily retrievable. This ensures that the data is readily available for both humans and computers. Furthermore, using clear naming conventions, relevant keywords, and specific data identifiers can aid users in efficiently finding and accessing the necessary data.

Typically, data will be stored on the server of the partner that generated it and shared according to the specific tasks outlined in the BEAMING work plan. Videos will be stored on the project's YouTube channel, and all other data will be stored on SharePoint. Partners should have backups of every data on external disks. The Coordinator backs up the deliverables.

The Data generated during the project can be categorised accordingly:

- *restricted data*: owned by the owner partner, the owner partner and the coordinator must store data in a repository during the project's lifetime and after for 5 years. (GA, Article 17, Decision 2015/444)
- *consortium data*: accessible to all consortium members and stored on the BEAMING SharePoint. Data must be kept for at least 5 years after the project ends.
- *open data*: accessible for the public and if it is possible, data will be published in a public repository. Open access is ensured in accordance with the requirements of the Grant Agreement (GA).

Open data will be shared through the BEAMING Data Management System. Selected datasets will be uploaded to trusted repositories (such as Zenodo, <https://zenodo.org/>) that comply with European Open Science Cloud (EOSC) requirements and will be managed according to the FAIR principles. These selected datasets will own a Digital Object Identifier (DOI) number for easy accessibility.

Article 17.4, Annex 5 of the GA states that beneficiaries must disseminate their results publicly as soon as possible, considering intellectual property, security, or legitimate interests (described in Section 4). They must give 15 days' notice to other beneficiaries before dissemination, who may object within 15 days if their interests are significantly harmed.

The General Principle for Dataset Naming

- Should be clear and descriptive,
- Use a consistent format,
- Avoid special characters,
- Short and concise but informative, and
- Use hyphens or underscores to separate words.

Dataset Naming

For datasets, the following naming should be used:

BEAMING_WPX_TX.X - [description of the activity] - [Partner acronym]

Deliverable Naming

For deliverables, the following naming should be used:

BEAMING DX.X - [Deliverable name] - [Partner acronym]

or

BEAMING DX.X - [Deliverable name] - [Partner acronym] - [version number]

3.2 Making Data Accessible

Data should be easily accessible to all partners. This necessitates storing data in a repository or data centre with proper access controls and security measures. Metadata should also clearly outline how to access the data. In the BEAMING project, Microsoft SharePoint is used (Section 2.3). The data-sharing process will be evaluated by the data

owner/creator and as specified by Section 4.5 of the Consortium Agreement (CA).

Additionally, all data collected for internal purposes will be stored in secure local repositories of the organisation responsible for collecting them and will be retained for 5 years after the end of the BEAMING project.

Moreover, the BEAMING project outputs will be made available to the public through the BEAMING website (<https://beamingproject.eu/>). Public documents like reports can be found under the documents tab. The project related news will be shared via the website (<https://beamingproject.eu/news/>), [newsletter](#), and [social media channels](#) (LinkedIn: <https://www.linkedin.com/company/beaming-project/>).

During the project BEAMING training program, e-learning materials will be developed and made publicly accessible on the BEAMING website. After the end of the project, the BEAMING website will remain a valuable resource for key stakeholders, further providing access to the developed e-learning materials. The training program tools will be available on the website throughout the project and for the additional two years after the project completion.

3.3 Making Data Interoperable

Data should be structured and formatted to facilitate easy integration with other data sources and systems. This involves using common data standards, formats, and vocabularies, which allow data to be combined and analysed across different domains and platforms. Standard vocabularies and formats will be used for data types in datasets during the BEAMING project. More detailed information will be provided in the updated DMP.

3.4 Increase Data Re-use

Data should be thoroughly documented and prepared for re-use. This entails providing clear and comprehensive metadata, detailing the

Funded by the European Union under grant agreement N° 101137131. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the Research Executive Agency (REA). Neither the European Union nor the granting authority can be held responsible for them.

data's provenance (origin and history), and specifying the terms and conditions for its use. These will be collected in the Data Summary Table (described in Section 2.2).

The BEAMING project has 46 Deliverables, and 39 of them are public (GA, List of Deliverables). They can be re-used after publishing.

4. Ethical and Legal Compliance

The commitment to legal and ethical principles is central to all research activities funded by the European Union. To ensure ethical compliance, the following measures, detailed in Sections 4.1 and 4.2, have been implemented.

The project will handle personal data, potentially including special categories of personal data. The legality of processing this data will be based on the informed, freely given, and unambiguous consent of the participants. Primarily, the processing of personal data will involve contact details and the opinions of stakeholders and experts who participate in the project's activities. The BEAMING project will handle personal data under the General Data Protection Regulation (EU) 216/679 (GDPR) (Section 4.2).

4.1 Intellectual Property Rights

In the BEAMING project, GA Article 16 describes Intellectual Property Rights (IPR), summarised below.

- Results are owned by the beneficiaries that generate them.
- If two or more beneficiaries jointly generate results, the results are jointly owned. This ownership structure applies to the research data generated in the BEAMING project.
- During the BEAMING project and for one year after its conclusion, dissemination of results by any party must adhere to specific procedures. These procedures are outlined in Article 17.4 of Annex 5 of the Grant Agreement (GA) and Section 8.4.2 of the Consortium Agreement (CA).

- Parties must provide 45 days' notice before any planned publication.
- Any objections to the planned publication must be made within 30 days.
- If no objections are made within this period, the publication is permitted.

4.2 General Data Protection Regulation

All personal data processed during the BEAMING project is protected under the General Data Protection Regulation (EU) 216/679 (GDPR). The GDPR is the cornerstone of European legislation, and ethical considerations are embedded in it. The GDPR must be fully applied across the EU as a binding legislative act. It applies whenever personal data is processed by organizations established in the EU, whether they function as processors or controllers. Under certain conditions, the GDPR also applies to companies outside Europe, such as when data processing activities involve offering goods or services (even if free) to data subjects in the EU or monitoring their behaviour. Although not all BEAMING partners in the BEAMING project are established in the EU, they are subject to GDPR rules.

The primary purpose of the GDPR is to protect natural persons regarding processing their personal data. Personal data refers to information about an identified or identifiable natural person ('data subject'). Personal data processed wholly or partly by automated means or in a non-automated manner intended to form part of a 'filing system' falls under the GDPR. However, only natural persons (including employees of businesses and public authorities) are protected by the GDPR.

In the BEAMING project, personal data processed is limited to contact information such as names, email addresses, and phone numbers. The relevant data subjects include employees of Consortium Partners involved in the project and individuals participating in the Project focus groups.

A dedicated legal partner with GDPR expertise will supervise personal data protection for the duration of the project and act as a "helpdesk" for the researchers (more details in Section 5.1).

Anonymisation and Pseudo-anonymisation of Personal Data

As in the GA task dedicated explicitly to ethics in WP1, we will put a particular effort into preparing informed consent explaining in a clear and detailed way how data will be collected, stored, and processed. Specific attention will be devoted to explaining the difference between anonymisation and pseudo-anonymisation to participants.

Anonymisation is the process of transforming data in such a way that individuals cannot be identified directly or indirectly. This involves removing or altering all personal identifiers, including names, addresses, and other information that could reveal someone's identity. Once data is anonymised, linking it back to an individual is no longer possible, making it exempt from data protection regulations. This ensures maximum privacy and security, as the risk of re-identification is practically eliminated. Partners should understand that anonymised data is highly secure and can be used freely for analysis and sharing without compromising individual privacy.

Pseudonymisation, on the other hand, involves replacing personal identifiers with unique codes or pseudonyms, while keeping the mapping between the original data and the pseudonyms in a separate, secure location. This process reduces the risk of identifying individuals directly. However, it does not eliminate it entirely, as the original data can still be re-identified if the pseudonymisation key is accessed. Pseudonymised data provides a balance between usability and privacy, allowing for detailed analysis while maintaining a level of confidentiality. Partners should recognize that while pseudonymised data is safer than raw data, it still requires careful handling and protection under data protection laws.

In the BEAMING project, personal/individual-related data will be processed in anonymised or pseudo-anonymised form where relevant.

5. Data security

The abovementioned procedures contribute to data protection, including SharePoint's two-factor authentication. Microsoft SharePoint adheres to comprehensive security practices and procedures (<https://learn.microsoft.com/en-us/purview/data-encryption-in-odb-and-spo#security-and-data-encryption-in-microsoft-365>).

5.1 Data Protection Officer

A Data Protection Officer (DPO) is essential for ensuring compliance with data protection laws and regulations, such as the GDPR. The DPO oversees the implementation of data protection policies, monitors compliance, and acts as a point of contact between the organization and regulatory authorities. By identifying and mitigating data protection risks, the DPO helps safeguard sensitive information, ensuring that personal data is handled responsibly and securely.

BEAMING Data Protection Officer's contact details are listed in Table 1. Table

1. Table Data Protection Officer

Project Data Protection Officer name	e-mail address
Dr Ágnes Frank	dpo@bme.hu

The coordinator will collect information from the Partners if their institution has an appointed DPO and if Data Protection Core is available for them. The collected information will be described in the updated DMP.

6. Conclusion

The DMP outlines how data will be handled throughout a project's lifecycle, detailing data collection, storage, protection, and sharing methods. It ensures that data is managed by best practices and regulatory requirements. The BEAMING DMP is a living document that will be updated twice during the project to reflect any changes or new developments, ensuring that data management strategies remain current and effective.

Further general information on Data Protection in the EU can be found on the link: https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_en