

HORIZON-WIDERA-2023-ACCESS-03

**BIOECONOMY EXCELLENCE ALLIANCE FOR STIMULATING
INNOVATIVE AND INCLUSIVE GREEN TRANSITION**

BEAMING

D2.2 – Updated Data Management Plan

Lead Contractor: BME

Author(s): Anikó Fehér, Susi Susanti, Balázs Imre

Date: 19/08/2026

This document corresponds to D2.2 of the BEAMING project (contract no. 101137131) and in particular to Work Package 2 (M19-48) led by the Budapest University of Technology and Economics (BME). It contains all relevant information regarding data management.

Project details			
Project acronym	BEAMING	Start/ Duration	1 January 2024 / 48 Months
Topic	HORIZON-WIDERA-2023-ACCESS-03-01	Call identifier	HORIZON-WIDERA-2023-ACCESS-03
Type of Action	HORIZON-CSA	Coordinator	BME
Contact persons	Balázs Imre (imre.balazs@edu.bme.hu) Anikó Fehér (feher.aniko@vbk.bme.hu)		
Website	beamingproject.eu		

Deliverable details			
Number	D2.2		
Title	Data Management Plan		
Work Package	WP2 – Project coordination and monitoring 2 nd phase		
Dissemination level	PU – Public	Nature	R – Document, report
Due date (M)	32	Submission date (M)	32
Deliverable responsible	1. BME	Contact person	Balázs Imre

Deliverable Contributors				
	Name	Org.	Role / Title	E-mail
Deliverable leader	Balazs Imre	BME	COO	imre.balazs@edu.bme.hu
Contributing Authors	Susi Susanti	BME	COO	susi.susanti@edu.bme.hu
	Anikó Fehér	BME	COO	feher.aniko@vbk.bme.hu
Reviewers	Boglárka Tóth	BME	BEN	toth.boglarka@bme.hu
	Liliya Pullman	FhG-ISI	BEN	liliya.pullmann@isi.fraunhofer.de
	Eleftheria Moraiti	CluBE	BEN	e.moraiti@clube.gr
Final review and quality approval	Balazs Imre	BME	COO	imre.balazs@edu.bme.hu
	Anikó Fehér	BME	COO	feher.aniko@vbk.bme.hu

Document History			
Date	Version	Name	Changes
08/08/2026	V0.1	First draft	first draft for internal review
10/08/2026	V0.2	Updated draft	Modified based on internal review
11/08/2026	V1.0	1 st version	Updated based on partners' comments
19/08/2026	V1.1	Final version	Minor changes during final review

Executive Summary

This updated Data Management Plan (DMP) describes the procedures and responsibilities for managing data generated and collected throughout the BEAMING project. Building upon the initial DMP submitted in Month 6, this version reflects the project's progress and provides updated information on data collection, storage, access, sharing, and compliance measures.

Since the beginning of the project, BEAMING has generated a diverse range of datasets, including survey responses, interview transcripts, workshop outputs, stakeholder engagement materials, institutional action plans, deliverables, training resources, dissemination materials, and other project documentation. The DMP provides an overview of these datasets through an updated Data Summary inventory describing their purpose, ownership, format, storage location, access conditions, and reusability potential.

The document further explains how the project applies the FAIR (Findable, Accessible, Interoperable and Reusable) principles and outlines the mechanisms used to ensure secure data storage, responsible data sharing, and long-term preservation where appropriate. Particular attention is given to the management of personal data, including informed consent procedures, anonymisation and pseudonymisation practices, restricted access arrangements, and compliance with the General Data Protection Regulation (GDPR) and Horizon Europe requirements.

As a living document, the DMP supports consistent and transparent data management across the consortium and will continue to be updated throughout the project lifecycle to reflect newly generated data, evolving practices, and emerging project needs.

Additional Elements in the Updated Version

Compared with the initial DMP (D1.3), the following sections have been updated to reflect the data generated and data management practices implemented during the project:

- **Section 1.1 – BEAMING Project:** updated with information on the project activities implemented to date and the main types of datasets already generated.
- **Section 1.2 – Why read a Data Management Plan?:** revised to clarify the role of the DMP as a living document and to reflect the transition from the initial data management framework to the management of datasets actually generated during project implementation.
- **Section 2 – Data Summary:** updated to establish the Data Summary as the central inventory of BEAMING datasets, regularly updated by consortium partners.
- **Section 2.2 – Data Structure, Metadata, and Documentation:** substantially updated with the completed Data Summary inventory.
- **Section 2.3 – Method and Tool of Data Collection:** updated to reflect the implemented use of the BEAMING SharePoint
- **Section 3.1 – Making Data Findable:** updated from planned to implemented practice regarding dataset and deliverable naming conventions; the naming rules defined in D1.3 are now reported as those used during project implementation.
- **Section 3.2 – Making Data Accessible:** updated to reflect actual availability of project outputs.
- **Section 3.3 – Making Data Interoperable:** substantially expanded with the file formats actually used within the project.
- **Section 3.4 – Increase Data Re-use:** updated with the actual status of project outputs.

- **Section 4.2 – General Data Protection Regulation:** expanded to reflect the personal data actually processed during implementation.
- **Anonymisation and Pseudonymisation of Personal Data:** expanded with information on how these procedures are applied in practice.
- **Section 5 – Data Security:** expanded to describe the technical and organisational data security measures.
- **Section 5.1 – Data Protection Officer:** revised to clarify the responsibility of individual partner institutions
- **Section 6 – Conclusion:** define the next steps.

Acronyms and Abbreviations

Acronyms	Explanation
CEE	Central-Eastern European
CA	Consortium Agreement
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 & Overview of the BEAMING project	9
1.1 BEAMING Project	9
1.2 Why read a Data Management Plan?	10
2. Data Summary	11
2.1 Purpose of the Data Collection.....	11
2.2 Data Structure, Metadata & Documentation	12
2.3 Methods & Tools of Data Collection	15
3. Making Data FAIR.....	15
3.1 Making Data Findable, Including Provisions for Metadata.....	16
3.2 Making Data Accessible	18
3.3 Making Data Interoperable	19
3.4 Increase Data Re-use	20
4. Ethical & Legal Compliance.....	21
4.1 Intellectual Property Rights.....	21
4.2 General Data Protection Regulation	22
4.3 Anonymisation & Pseudo-anonymisation of Personal Data	23
5. Data security	25
5.1 Data Protection Officer	26
6. Conclusion.....	27

1. Introduction & Overview of the 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 emphasises 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



Funded by the
European Union

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.

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.

Since the start of the project, BEAMING has implemented a wide range of activities supporting capacity building, stakeholder engagement, institutional transformation, and bioeconomy research collaboration. These activities have generated various datasets, including survey responses, interview transcripts, workshop outputs, training materials, institutional action plans, dissemination materials, and project deliverables. The management of these datasets is addressed in the present updated Data Management Plan.

1.2 Why read a Data Management Plan?

The Data Management Plan (DMP) is a living document that is updated throughout the lifetime of the BEAMING project to reflect newly generated data, evolving data management practices, and emerging legal, ethical, and technical requirements. This updated version builds on the initial DMP and incorporates information on datasets generated during project implementation, including research, stakeholder engagement, training, communication, dissemination, and project management activities.

The DMP provides guidance to all consortium partners on the collection, documentation, storage, sharing, protection, and preservation of project data. By following these procedures, partners can ensure that project data are managed consistently and in accordance with FAIR principles, Horizon Europe requirements, and applicable data protection regulations, including the General Data Protection Regulation (GDPR).

2. Data Summary

This section provides a comprehensive overview of the data generated and utilised 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 data produced during the BEAMING project are summarised in the Data Summary table. More details are provided in Section 2.2.

The Data Summary table serves as the central inventory of project datasets and is regularly updated by consortium partners to ensure consistent documentation and compliance with FAIR principles and Horizon Europe requirements.

2.1 Purpose of the Data Collection

The primary purpose of data collection in the BEAMING project is to support the implementation, monitoring and evaluation of the project activities and objectives. Data are collected to assess the capacities, needs and practices of participating higher education institutions and their innovation ecosystems; to inform institutional transformation and capacity-building activities; and to support the development of strategies and actions related to knowledge valorisation, Open Science, collaboration and stakeholder engagement.

By systematically collecting and analysing relevant quantitative and qualitative data, BEAMING can identify institutional needs, gaps, good practices and changes over time, provide an evidence base for project interventions and recommendations, and monitor progress towards the expected project outcomes. The collected data therefore support

evidence-based decision-making within the project and contribute to evaluating the effectiveness and impact of BEAMING activities.

Additionally, collecting data from partners will help identify gaps, trends, needs and opportunities within HEIs in Widening and Associated Countries active in bioeconomy research, 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 and Associated Countries, promote effective technology and know-how transfer, and strengthen collaboration across EU Member States and Associated Countries.

2.2 Data Structure, Metadata & 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** 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, questionnaires, interviews and focus groups reports, deliverables, action plans, strategic documents, workshops and webinars, training materials and related documentation, participant and contact lists, presentations, videos, 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 has been collected from partners during the project and included in this updated DMP. As this deliverable is publicly available, the complete Data Summary inventory is not included in the present document. The detailed inventory may contain personal, sensitive, confidential, or institution-specific information and is therefore maintained as an internal project document on the BEAMING SharePoint, accessible to authorised consortium members. To provide a transparent overview of the data generated by the project

without disclosing restricted information, an aggregated summary of the registered datasets by category is presented below.

As of Month 32, the BEAMING Data Summary inventory contains 373 registered datasets and information assets generated across project activities. Several entries represent collections of institution-specific datasets submitted by participating BEAMING HEIs.

Table 1. Statistical Overview of Registered Datasets

Dataset Category	Number of Datasets
Deliverables	28
Institutional Action Plans	16
Workshop minutes/reports	28
Focus group reports	10
Survey Datasets	62
Interview Datasets	91
Training Modules	8
Contact Lists	7
Newsletters	10
Press releases	2
Dissemination Materials	6
Project website	1
Kick-off meeting reports	2
Data monitoring	6
Mobility reports	26
Presentation materials	41
PP Inputs	17
Videos	5
Other Project Documentation	7
Total	373

2.3 Methods & Tools of Data Collection

In the BEAMING project, data collection is systematically organised 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 authorised 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 organisation 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 emphasise Fairness, Accessibility, Interoperability, and Reusability of data. These principles are intended to facilitate data exchange and maximise 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, organisations and institutions can improve the discoverability, accessibility, and usefulness of their data, thereby driving scientific progress, economic growth, and societal benefits. The



Funded by the
European Union

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.

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 all data on external disks. The Coordinator backs up the deliverables.

The Data generated during the project can be categorised accordingly:

- *restricted data*: data that cannot be made publicly available due to personal data protection, confidentiality or other legitimate restrictions. Such data remain under the responsibility of the partner that generated or collected them and are stored in secure institutional storage systems and/or in access-controlled areas of the BEAMING SharePoint, as appropriate. Access is limited to authorised persons in accordance with the applicable data protection, confidentiality and Consortium Agreement requirements. Restricted data are retained for the period required by the Grant Agreement, applicable legal requirements and/or the relevant institutional policies.

- *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 are published in a public repository. Open access is ensured in accordance with the requirements of the Grant Agreement (GA).

As of Month 32, no project datasets have been assigned a Digital Object Identifier (DOI) and no datasets have yet been deposited in an external trusted repository. During the remaining project period, the consortium will review the datasets registered in the BEAMING Data Summary inventory to identify those suitable for public sharing and reuse. Research datasets that can be made openly available, taking into account data ownership, consent conditions, confidentiality, intellectual property rights and data protection requirements, will be deposited in a trusted repository, such as Zenodo, in accordance with the FAIR principles and the requirements of the Grant Agreement. Where open access cannot be provided, the reasons for restricting access will be documented in the Data Summary and, where relevant, reflected in the final DMP. Public project outputs that do not constitute research datasets will continue to be made available through the BEAMING website and other appropriate dissemination channels.

The dissemination of project results follows the procedures and requirements set out in Article 17 and Annex 5 of the Grant Agreement and Section 8.4 of the Consortium Agreement, taking into account intellectual property rights, confidentiality, security and other legitimate interests.

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 was used:

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

Deliverable Naming

For deliverables, the following naming was 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 are 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 are 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 have been 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 were 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 were used for data types in datasets during the BEAMING project.

Within the BEAMING project, commonly used and widely supported file formats are applied whenever possible to facilitate data exchange and long-term preservation. Typical formats include XLSX and CSV for survey and monitoring data, DOCX and PDF for reports, action plans and deliverables, PPTX and PDF for training and presentation materials, and JPG, PNG and MP4 formats for visual and multimedia content.

Standardised documentation is supported by common project templates and the Data Summary Table used across the consortium. The Data Summary records common metadata fields for project datasets, including title, keywords, related WP and task, data source, collector, data type and format, storage location, access and sharing conditions, and reusability. These common fields facilitate the

consistent documentation and interpretation of datasets generated by different project activities and partners.

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 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, of which 39 are public (GA, List of Deliverables). As of Month 32, 30 deliverables have been completed and submitted including 24 public deliverables that have been published through the BEAMING project website. These publicly available deliverables represent an important source of reusable project knowledge and provide access to project findings, methodologies, case studies, guidelines, roadmaps, training resources, and other outputs generated throughout the project. In addition to deliverables, selected open-access materials such as training modules, newsletters, press releases, dissemination resources, and website content may also be reused by researchers, higher education institutions, policymakers, innovation actors, and other stakeholders, subject to any applicable copyright, attribution, or project-related requirements.

4. Ethical & 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) 2016/679 (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 within the BEAMING project are handled in accordance with applicable data protection legislation, including the General Data Protection Regulation (EU) 2016/679 (GDPR), where applicable, as well as the data protection obligations set out in the Grant Agreement and Consortium Agreement. All partners, including those established outside the EU, are required to comply with the data protection requirements applicable to their participation in the project and with relevant national legislation.

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, phone numbers, institutional affiliations, professional positions, workshop registrations, participation records, stakeholder opinions, survey responses, interview contributions, and other information voluntarily provided by participants. Such data are collected only where necessary for project implementation and are processed according to the principles of lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity, and confidentiality.

For activities involving the collection of personal data directly from participants, such as surveys, interviews, and focus groups, informed consent is obtained where consent is used as the applicable legal basis



for processing. Participants are informed about the purpose of the data collection, the types of personal data being processed, storage arrangements, access rights, and their rights as data subjects under the GDPR.

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).

4.3 Anonymisation & 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.

Anonymised data generally reduce privacy risks and can facilitate further analysis and sharing. However, in small stakeholder samples, particularly in qualitative interviews involving specific institutions or professional roles, a risk of indirect re-identification may remain even after direct identifiers have been removed. Therefore, anonymised data are assessed on a case-by-case basis before sharing, and additional

measures, such as aggregation or removal of potentially identifying contextual information, are applied where necessary.

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.

Within BEAMING, anonymisation and pseudonymisation practices are applied where appropriate, particularly for survey datasets, workshop feedback, and other stakeholder engagement activities. Personal identifiers are removed or restricted whenever individual-level information is not required for project implementation, analysis, reporting, or monitoring purposes. Access to non-anonymised datasets is limited to authorised personnel and data owners, and any sharing of project results is undertaken in aggregated or anonymised form whenever possible.

In the BEAMING project, personal/individual-related data are processed in anonymised or pseudo-anonymised form where relevant, while ensuring compliance with GDPR requirements, participant consent conditions, and institutional data protection policies.

5. Data security

Data security within BEAMING is ensured through a combination of technical and organisational measures. The BEAMING SharePoint serves as the main shared data storage and collaboration environment and access is restricted to authorised consortium members. User authentication, including two-factor authentication, contributes to preventing unauthorised access. Access to project data is granted according to users' roles and involvement in project activities, while personal, confidential or otherwise restricted data are accessible only to authorised personnel.

Where project data are stored locally by partners, the responsible institution applies its own institutional data security, access control and backup procedures. Partners are responsible for maintaining appropriate backups of the data they generate and for preventing unauthorised access, accidental loss, alteration or disclosure. Personal and sensitive data are stored with appropriate access restrictions, and anonymisation or pseudonymisation is applied where relevant to reduce data protection risks.

Microsoft SharePoint applies security and data-encryption measures for data stored within the platform. The consortium will continue to review access rights and data storage arrangements throughout the project and will address any identified data security risks in accordance with applicable institutional policies and project requirements.

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 organisation 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.

Each BEAMING partner is responsible for ensuring compliance with the data protection requirements applicable to its project activities and follows its institutional data protection procedures. Where an institution has an appointed Data Protection Officer (DPO), the institutional DPO provides guidance and support on data protection matters in accordance with the institution's procedures.

At the coordinating institution (BME), data protection matters can be referred to the institutional Data Protection Officer:

Dr Ágnes Frank

E-mail: dpo@bme.hu

The Coordinator supports consortium-level data protection coordination, while responsibility for the lawful processing and protection of personal data remains with the respective partner institutions in accordance with their applicable legal and institutional requirements.

6. Conclusion

The BEAMING Data Management Plan (DMP) provides a framework for the effective management of data generated throughout the project. Since the start of the project, BEAMING has produced a wide range of datasets and information assets, including survey and interview datasets, workshop and focus group reports, institutional action plans, training modules, project deliverables, dissemination materials, newsletters, mobility reports, contact lists, and other project documentation. These datasets are documented through the BEAMING Data Summary table, which supports consistent data management across all work packages and consortium partners.

This updated DMP reflects the project's progress up to Month 32 and describes the procedures implemented to ensure that data are managed in accordance with the FAIR principles and relevant ethical and legal requirements. Dataset documentation, metadata management, controlled access procedures, and secure storage arrangements support the findability, accessibility, interoperability, and reusability of project data where appropriate. Public project outputs are disseminated through the BEAMING website, while datasets containing personal, confidential, or institution-specific information are subject to appropriate access restrictions and GDPR-compliant protection measures.

As a living document, the DMP will continue to be updated throughout the remaining project duration to reflect newly generated datasets, evolving data management practices, and any additional project requirements. Through these measures, BEAMING aims to ensure transparent, responsible, and sustainable management of project data while maximising the long-term value and impact of the knowledge and resources generated by the project.

During the remaining project period, particular attention will be given to reviewing the Data Summary inventory and identifying research datasets suitable for deposition in trusted repositories and long-term

reuse. The outcomes of this review, including repository information and any justified access restrictions, will be reflected in the final DMP.

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



Funded by the
European Union

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.