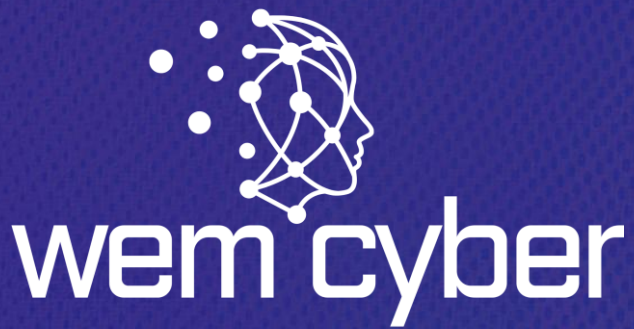




D1.3

DATA MANAGEMENT PLAN

Contact

coo.wemcyber@bilisimvadisi.com.tr



Funded by
the European Union

D1.3

DATA MANAGEMENT PLAN

WEM Cyber

Widening Excellence and Mentoring In Cybersecurity

CALL: HORIZON-WIDERA-2024-TALENTS-03

TYPE OF ACTION: HORIZON-CSA

STARTING DATE: 1 JANUARY 2026

DURATION: 36 MONTHS

COORDINATOR: BILISIM VADISI TEKNOPARK YONETICI AS

DATE

June 2026 M6

WORK PACKAGE

WP1

LEADER

Université de Toulouse

DISSEMINATION LEVEL

Public

TYPE

Document, report



**Funded by
the European Union**

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

© Copyright 2026 WEM Cyber. This document may not be copied, reproduced, or modified in whole or in part for any purpose without written permission from WEM Cyber. In addition to such written permission to copy, reproduce, or modify this document in whole or part, an acknowledgement of the authors of the document and all applicable portions of the copyright notice must be clearly reference. All rights reserved.

Authors

Lili Nemec Zlatolas
Saša Grašič

Organisation

University of Maribor
University of Maribor

Peer Reviews

Nuria Costa
Bilgin Metin
Jūratė Janutėnaitė–Bogdanienė

Organisation

Universitat Pompeu Fabra
Boğaziçi University
Vilnius Gediminas Technical University

Revision History

VERSION	DATE	REVIEWER	MODIFICATIONS
0.0	10/04/2026		First version
1.0	28/05/2026	Peer reviews listed above	Modifications considering reviewers comments
2.0	24/06/2026	Peer reviews listed above	Modifications considering reviewers comments
3.0	28/06/2026	Peer reviews listed above	Modifications considering reviewers comments



Funded by
the European Union

ABBREVIATIONS AND ACRONYMS

Abbreviation	Meaning
BU	Boğaziçi University
BV	Bilisim Vadisi Teknopark Yonetici AS
CC0	Creative Commons Zero
Cloudmetrik	Cloudmetrik Teknoloji Anonim Sirketi
CSA	Coordination and Support Action
Cyberwhiz	Cyberwhiz Siber Guvenlik Anonim Sirketi
DMP	Data Management Plan
DOI	Digital Object Identifier
FAIR principles	Data should be Findable, Accessible, Interoperable, and Reusable
GDPR	General Data Protection Regulation
Oninc	Oninc Elektronik As
PID	Persistent identifier
SCCs	Standard Contractual Clauses
SecroMix	SMSK Bilgi Teknolojileri ve Ticaret Limited Sirketi
SphereTech	Spheretech Yazilim Anonim Sirketi
UBITECH	Gioumpitek Meleti Schediasmos Ylopoiisi Kai Polisi Ergon Pliroforikis Etaireia Periorismenis Efthynis
UM	Univerza v Mariboru
UPF	Universidad Pompeu Fabra
UT	Université de Toulouse
VT	Vilnius Gediminas Technical University
W4C	Women4Cyber Mari Kert – Saint Aubyn Foundation



Funded by
the European Union

CONTENTS

INDEX OF TABLES	6
EXECUTIVE SUMMARY	7
INTRODUCTION	8
1. DEFINITIONS	9
1.1. FAIR Principles	9
1.2. Data definition	9
2. DATA SUMMARY	11
2.1. Re-use of existing data	11
2.2. Types and formats of data generated or re-used	11
2.3. Purpose of data generation or re-use	12
2.4. Expected size of the data	13
2.5. Origin and provenance of data	13
2.6. Mapping of Data to Work Packages	13
2.7. Data utility	15
2.8. Data handling	15
3. FAIR PRINCIPLES.....	17
3.1. Making data findable, including provisions for metadata	17
3.2. Making data accessible.....	18
3.3. Making data interoperable	20
3.4. Increase data re-use	21
4. OTHER RESEARCH OUTPUTS.....	23
4.1. Management of research outputs.....	23
4.2. Accessibility and sharing	23
4.3. Application of FAIR principles	24
4.4. Re-use and long-term availability	24
5. ALLOCATION OF RESOURCES	25
5.1. Costs of data and research output management	25
5.2. Coverage of costs.....	25



Funded by
the European Union

5.3.	Responsibilities for data management.....	25
5.4.	Long-term preservation	26
6.	DATA SECURITY	28
6.1.	Data security measures	28
6.2.	Data recovery and continuity.....	28
6.3.	Secure storage and long-term preservation.....	29
6.4.	Protection of sensitive data	29
6.5.	Data breach response	29
6.6.	Data retention	30
7.	ETHICS	31
7.1.	Ethical and legal considerations	31
7.2.	Informed consent	32
7.3.	Artificial intelligence and data use	32
8.	OTHER ISSUES.....	34
	CONCLUSION	35
	REFERENCES	36

INDEX OF TABLES

Table 1 – Categories of generated data	14
--	----



Funded by
the European Union

EXECUTIVE SUMMARY

This Data Management Plan (DMP) outlines the strategy, procedures, and responsibilities for the management of data and other research outputs generated within the WEM Cyber project. The document is prepared in accordance with Horizon Europe requirements and aligns with the FAIR principles, ensuring that data is Findable, Accessible, Interoperable, and Reusable [1], while also addressing security, ethical, and legal considerations.

WEM Cyber is a Coordination and Support Action aimed at strengthening cybersecurity capacity, fostering knowledge exchange, and promoting gender inclusion through training, mentoring, and secondment activities. As such, the project generates a diverse range of data types, including personal and administrative data, training materials, dissemination outputs, and project management documentation. The DMP defines how these data will be handled throughout their lifecycle, from generation and processing to storage, sharing, and long-term preservation.

The project adopts a balanced approach to data openness, ensuring that publicly shareable outputs are made available through trusted repositories such as Zenodo [2], while sensitive data, including personal and cybersecurity-related information, is protected through appropriate technical and organisational measures. Particular attention is given to compliance with the General Data Protection Regulation (GDPR) [3], including the handling of personal data and cross-border data transfers involving non-EU partners.

In addition to data, the DMP also addresses the management of other research outputs, such as training materials, methodologies, and best practices, ensuring that they are documented, accessible, and reusable as defined in this DMP.

The project fully supports Horizon Europe open science principles by ensuring timely and transparent access to publicly available research outputs.

This DMP is a living document and will be updated throughout the project lifecycle to reflect evolving requirements, project developments, and best practices in data management.

INTRODUCTION

The WEM Cyber project (Widening Excellence and Mentoring in Cybersecurity) is a Horizon Europe Coordination and Support Action that aims to enhance cybersecurity capacity across Europe, with a particular focus on widening countries and the promotion of gender inclusion in the cybersecurity domain.

The project brings together academic institutions and industry partners to implement training programmes, secondments, and mentoring and coaching activities that support knowledge transfer and skills development. These activities generate a variety of data and research outputs that must be managed in a structured, secure, and compliant manner.

This Data Management Plan defines the framework for handling all data and research outputs generated or reused within the project. It follows the requirements set out in the Horizon Europe Grant Agreement and reflects best practices in research data management, including the application of the FAIR principles.

The DMP covers the full data lifecycle, including data generation, processing, storage, sharing, and preservation. It also addresses key aspects such as metadata provision, accessibility, interoperability, reusability, data security, ethical considerations, and long-term preservation. In addition, it considers the management of other research outputs beyond data, ensuring a comprehensive approach to knowledge management within the project.

Given the nature of the project, particular attention is paid to the handling of personal data and potentially sensitive information related to cybersecurity activities. The DMP therefore

The approach described in this Data Management Plan ensures that all data generated within the project is systematically identified, managed, and governed in a consistent and controlled manner across all work packages. The document is intended to serve as a practical guide for all project partners and will be updated as necessary throughout the project duration.



Funded by
the European Union

1. DEFINITIONS

For the purposes of this document, important terms are defined below and are used consistently throughout the Data Management Plan.

1.1. FAIR Principles

The WEM Cyber project applies the FAIR principles (Findable, Accessible, Interoperable, Reusable) [1] as a core component of its data management strategy:

- **Findable:** Data and research outputs will be described using appropriate metadata and, where applicable, assigned persistent identifiers (e.g. DOIs) to ensure they can be easily discovered and cited.
- **Accessible:** Publicly available outputs will be shared through trusted open-access repositories such as Zenodo [2], while restricted data will remain protected with metadata available to ensure transparency.
- **Interoperable:** Data will be stored in widely used, non-proprietary formats (e.g. PDF, CSV) and, where relevant, aligned with common standards to enable integration and reuse.
- **Reusable:** Data and outputs will be accompanied by sufficient documentation and, where possible, shared under open licences (e.g. Creative Commons) to support long-term reuse.

1.2. Data definition

For the purposes of this Data Management Plan, the term “data” encompasses research data, other research outputs, and operational data generated through project activities and digital platforms:

- **Research data** refers to data collected or generated to support the analysis, evaluation, and reporting of project activities. This includes, for example, participant-related data (e.g. applications, profiles, evaluation data), survey responses, and monitoring data related to training and secondments. This also includes aggregated or system-generated data derived from the use of project platforms, where applicable.
- **Other research outputs** include materials that are not datasets but contribute to the project objectives, such as training materials, methodological frameworks, reports, publications, and content developed through the Knowledge Transfer Platform. These outputs are managed and shared in line with the same principles of



Funded by
the European Union

accessibility, transparency, and reuse, while respecting legal, ethical, and confidentiality requirements.



**Funded by
the European Union**

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101216854

2. DATA SUMMARY

In this section, we will explain what type of data will be used in the project and explain the generated or re-used data.

2.1. Re-use of existing data

The WEM Cyber project is a Coordination and Support Action (CSA) and does not primarily rely on the reuse of large-scale pre-existing research datasets. However, the project builds upon and reuses existing knowledge resources, including established training materials, methodological frameworks, and best practices in the field of cybersecurity capacity building and skills development.

In particular, the project leverages:

- Existing training methodologies and educational resources in cybersecurity,
- Established mentorship programme frameworks (e.g. Women4Cyber initiatives),
- State-of-the-art scientific and technical knowledge in relevant cybersecurity domains, such as artificial intelligence in cybersecurity, post-quantum cryptography, and Zero Trust architectures.

The reuse of such resources serves to ensure efficiency, avoid duplication of effort, and align project activities with current scientific and industrial practices.

The project does not foresee the reuse of sensitive or restricted external datasets, as its primary focus lies in training, mentoring, and knowledge exchange rather than experimental data analysis. Where reuse of existing datasets has been considered, it has been limited to publicly available or non-sensitive materials due to data protection, confidentiality, and relevance considerations.

2.2. Types and formats of data generated or re-used

The project will generate a variety of data types, reflecting its multidisciplinary nature and focus on training, secondments, and coordination activities.

The main categories of data include:

- Personal and administrative data. This includes participant-related information such as application data, CVs, profiles, and evaluation forms, as well as data collected through skills assessments and feedback mechanisms.
- Training and dissemination materials. Training content, presentations, reports, and educational resources will be developed and shared within the consortium and with external stakeholders. In addition, recordings of training sessions and workshops will be produced.



Funded by
the European Union

- Project management and monitoring data. This includes internal documentation, progress reports, performance indicators, and evaluation data related to secondments and project activities.
- Research-related outputs. Outputs generated during secondments and collaborative activities, including reports, analyses, and best practices, will also constitute part of the project data.
- Platform-related data. Data generated through the Knowledge Transfer Platform, including uploaded content, metadata, and user interaction data. The Knowledge Transfer Platform processes uploaded content, associated metadata, user interaction data (e.g. usage and feedback), while user account data and technical system data are managed by the platform provider (Sploro).

The DMP defines which data will be openly accessible and which will remain confidential, establishing a framework that supports long-term reuse while ensuring that data can be easily located, accessed, and used by relevant stakeholders.

The data will be stored in commonly used and widely accessible formats, including structured formats (e.g. CSV, XLSX), textual documents (e.g. DOCX, PDF), presentation formats (e.g. PPTX), and multimedia formats (e.g. video recordings).

These data categories are consistent with the project's research data management approach and planned activities.

2.3. Purpose of data generation or re-use

The generation and use of data within the WEM Cyber project are directly linked to its core objectives, namely strengthening cybersecurity capacity, enhancing research and innovation potential, and promoting gender inclusion in the cybersecurity domain.

Data is generated and used to:

- Monitor project performance and ensure effective coordination (WP1).
- Support the implementation and evaluation of secondments (WP2).
- Enable personalised training and skills development programmes (WP3).
- Facilitate mentorship and coaching activities (WP3).
- Enable knowledge sharing through the Knowledge Transfer Platform (WP3).
- Support dissemination, communication, and impact activities (WP4).

Through these activities, data contributes to improving competencies, supporting career development, and fostering collaboration between academia and industry.



Funded by
the European Union

2.4. Expected size of the data

The WEM Cyber project is not expected to generate large-scale datasets. The overall volume of data is anticipated to be moderate and consistent with the nature of a Coordination and Support Action.

The main contributors to data volume include:

- Documentation and reports (moderate volume).
- Training materials and educational content (moderate volume).
- Multimedia recordings of training sessions (potentially larger volume within the overall dataset).
- Structured datasets from surveys and evaluations (limited volume).

Overall, the total data volume is expected to remain within a low-to-medium range (in the order of several gigabytes over the project duration).

2.5. Origin and provenance of data

The data generated within the project originates from multiple sources, including:

- Project participants and applicants (e.g. personal data, feedback, evaluation data).
- Consortium partners (e.g. reports, training materials, dissemination outputs).
- Secondment activities (e.g. research outputs, analyses, documentation).
- The Knowledge Transfer Platform (e.g. uploaded materials, usage data).
- External publicly available sources (e.g. scientific publications, existing methodologies).

The project explicitly acknowledges that it will handle both personal data and research-related outputs, and that such data will be managed in accordance with GDPR requirements and FAIR principles.

2.6. Mapping of Data to Work Packages

To ensure clarity and traceability, the main categories of data generated within the project are linked to specific Work Packages as follows in Table 1.

D1.3 DATA MANAGEMENT PLAN

Table 1 – Categories of generated data

Work Package / Source	Type of Data	Sensitivity level	Storage Location	Sharing Level	Responsibility Entity
WP1 – Project Management	Administrative data, reports, financial claims, procedures, metadata	Low / Personal	SharePoint (secure environment)	Internal	Partners (data owners); BV (GDPR oversight); UM (guidance)
WP2 – Secondments	Applications, CVs, evaluation data, secondment records	Personal / Sensitive	Sploro platform and SharePoint	Restricted (not publicly shared)	Partners (data owners); BV (Lead DPO); UM (guidance)
WP3 – Training & Mentoring	Training materials, feedback data, recordings	Mixed	SharePoint and Knowledge Transfer Platform (UBITECH)	Public (if non-personal) / Restricted	Partners; BV (ethical oversight)
WP4 – Dissemination	Publications, reports, communication materials	Public	SharePoint + Knowledge Transfer Platform (UBITECH) + Zenodo + Project website (W4C)	Open access	Partners (owners); BV (compliance); UM (support)
WP5 – Ethics & Compliance	Consent forms, ethics reviews, SCCs, compliance records	Personal / Sensitive	SharePoint	Restricted	BV (Lead DPO); UM (validation/support)
Knowledge Transfer Platform	Uploaded content, metadata, user interaction data	Mixed	UBITECH	Aggregated / anonymised only	UBITECH (platform); Partners (content); BV (oversight)
Project Website	Public dissemination content	Public	Website hosting platform	Open access	Partners; BV (compliance support)

Sensitivity levels used in the Table 1 are defined as follows:

- **Public:** Data intended for open access without restrictions.
- **Low:** Non-sensitive internal data with minimal confidentiality requirements.
- **Mixed:** Data containing both non-personal and potentially sensitive elements, requiring controlled access and possible anonymisation.
- **Personal / Sensitive:** Data containing personal information or sensitive content, subject to strict GDPR protection and restricted access.

Data classification is the responsibility of the data-owning partner, with oversight from BV (Lead DPO) and guidance provided by UM. This mapping ensures that data management procedures are consistently applied across all project activities.

2.7. Data utility

The data generated within the WEM Cyber project is expected to be of value to a wide range of stakeholders beyond the project consortium.

Potential users include:

- Academic institutions, for the development of training programmes and curricula.
- Industry stakeholders and SMEs, for skills development and innovation in cybersecurity.
- Policy makers and European initiatives, for evidence-based decision-making and addressing skills gaps.
- The broader cybersecurity community, through access to best practices and open materials.
- Future research projects, through reuse of methodologies and training resources.

Where appropriate, data and project outputs will be made available through open access repositories, the project's Knowledge Transfer Platform, and dissemination activities, ensuring maximum visibility and impact.

2.8. Data handling

Data generated within the project will follow a structured lifecycle, ensuring consistency, traceability, and compliance with ethical and legal requirements. The lifecycle includes:

1. Data collection or creation within work packages.
2. Storage in secure environments (e.g. SharePoint, Knowledge Transfer Platform, institutional systems, or subcontractor platforms).
3. Internal review and validation by responsible partners.
4. Application of data protection techniques.
5. Publication of eligible outputs in open-access repositories (e.g. Zenodo).



Funded by
the European Union

6. Long-term preservation of data and research outputs in trusted repositories and institutional systems. Public outputs will be preserved in repositories such as Zenodo, while restricted data will be retained in secure institutional environments for a minimum period of five years after the end of the project, in accordance with Horizon Europe and GDPR requirements.

Special attention is given to data protection processes. Data handling includes anonymisation, pseudonymisation, aggregation, and data minimisation, applied in accordance with GDPR principles. Reports and outputs will be anonymised where required prior to sharing or publication.

Platform-related data will be processed within the Knowledge Transfer Platform managed by UBITECH, which is responsible for implementing internal data processing mechanisms. UM does not take an administrative or operational role on this platform.

The Knowledge Transfer Platform will remain operational for the duration of the project and for a period thereafter as defined by project sustainability planning. The technical maintenance and operation of the platform are the responsibility of UBITECH, while partners remain responsible for the content they upload. Where necessary, important outputs will be transferred to trusted repositories to ensure long-term availability.

Data uploads to shared environments will be coordinated by BV where necessary, while partners remain responsible for the content and correctness of the data they provide.

This structured approach ensures that data is managed in a controlled, auditable, and compliant manner throughout its lifecycle.

3. FAIR PRINCIPLES

The WEM Cyber project is committed to implementing the FAIR principles [1] to ensure that all data and research outputs are findable, accessible, interoperable, and reusable, as further explained in this chapter.

3.1. Making data findable, including provisions for metadata

3.1.1. Persistent identifiers

As defined in this DMP, data and research outputs generated within the WEM Cyber project will be assigned persistent identifiers (PIDs) to ensure long-term findability and citability. In particular, publicly available deliverables, publications, and selected datasets will be deposited in trusted open-access repositories (e.g. Zenodo), which automatically assign Digital Object Identifiers (DOIs).

For internal project data stored within the consortium (e.g. working documents, administrative data, or restricted datasets), persistent identifiers will not systematically be assigned. However, such data will be organised using consistent naming conventions and version control within the project's SharePoint environment to ensure traceability and internal findability. A project-wide naming convention has been agreed, following the format DX.X_VersionNumber_Date (e.g. D4.1_V1.0_20260302).

3.1.2. Metadata standards and provision of rich metadata

The WEM Cyber project will ensure that all publicly shared data is accompanied by rich and structured metadata to facilitate discovery, access, and reuse.

Metadata will be created at different levels, depending on the type of data:

- For publications and datasets deposited in repositories metadata will follow the standards required by the selected repository (e.g. Zenodo). These typically include title, authors and affiliations, description/abstract, publication date, keywords, funding information (Horizon Europe grant reference), licensing conditions.
- For internal project data (SharePoint environment) metadata will be implemented through structured folder hierarchy, file naming conventions, document versioning, basic descriptive fields (e.g. author, date, WP, document type).

In domains where no specific disciplinary metadata standards are required (as is the case for most coordination, training, and administrative data), the project will rely on general-purpose metadata standards and best practices, ensuring consistency and clarity across all data types.



Funded by
the European Union

3.1.3. Metadata harvesting and indexing

Metadata associated with publicly available datasets and publications will be made available in a format that supports harvesting and indexing by external systems. In particular:

- Data deposited in open repositories (e.g. Zenodo) will be exposed via standard protocols (e.g. OAI-PMH), enabling indexing by OpenAIRE, Google Scholar, other academic and research discovery platforms.
- Metadata will be openly accessible even in cases where the underlying data is restricted, ensuring that the existence and characteristics of the data remain discoverable.

This approach ensures compliance with Horizon Europe open science requirements and maximises the visibility and potential reuse of project outputs.

3.2. Making data accessible

3.2.1. Repository

The WEM Cyber project will ensure that all publicly available research outputs and relevant datasets are deposited in trusted and recognised open-access repositories.

In particular, the project will use Zenodo (operated by CERN and supported by OpenAIRE), which is fully compliant with Horizon Europe requirements

Only data that is suitable for public dissemination (i.e. non-sensitive and non-confidential data) will be deposited in such repositories.

The project will also ensure alignment with Horizon Europe open access requirements and consortium agreement provisions on data sharing and intellectual property.

The selected repository (Zenodo) ensures that all deposited datasets and publications are assigned persistent identifiers (Digital Object Identifiers – DOIs).

These identifiers provide a permanent and unique reference to each dataset or publication, resolve directly to the corresponding digital object, and ensure long-term accessibility and citability.

The repository guarantees that each DOI is resolvable via standard web protocols and that metadata remains accessible even if access to the underlying data is restricted.

This approach ensures that all publicly shared outputs of the WEM Cyber project are easily accessible, reliably identifiable and compliant with FAIR principles and Horizon Europe requirements.

3.2.2. Data

The WEM Cyber project is committed to the principles of open science and will make data openly available wherever possible. Public deliverables, scientific publications, and non-sensitive datasets will be deposited in trusted open-access repositories such as Zenodo, in accordance with Horizon Europe requirements.

However, not all data generated within the project can be made openly available. Restrictions apply primarily due to legal, contractual, and project-specific considerations. In particular, personal data collected from participants (e.g. applications, CVs, evaluation data, and mentoring records) will not be shared publicly in order to ensure compliance with the General Data Protection Regulation (GDPR) and to protect the privacy of individuals.

In addition, certain data may be subject to confidentiality obligations under the Consortium Agreement or related to the legitimate interests of project partners, particularly in the context of secondments involving industry. Furthermore, some cybersecurity-related content may require controlled access due to its potentially sensitive nature.

Where appropriate, limited embargo periods may be applied to allow time for publication or, where relevant, the protection of intellectual property. Such embargoes will be justified on a case-by-case basis and kept as short as possible, in line with the principle that research data should be made available without undue delay.

All publicly available data will be accessible through free and standardised protocols, primarily via HTTP/HTTPS access provided by open repositories such as Zenodo. These repositories ensure that data is accessible in a consistent, interoperable, and machine-readable manner.

Data that cannot be made openly available will be stored in secure environments (e.g. SharePoint, Sploro secondments platform, Knowledge Transfer Platform, project website) and accessed only by authorised users. During the project, access will be granted based on defined roles and responsibilities within the consortium. After the end of the project, access to restricted data may be granted upon justified request, subject to legal, ethical, and contractual constraints, and with the approval of the data-owning partner.

Access to restricted data will be managed through secure authentication mechanisms, including Microsoft 365-based access control systems. Role-based permissions will ensure that only authorised individuals can access specific datasets, and that access is traceable and auditable. Data access will be governed through clearly defined responsibilities within the consortium and oversight by the Ethics Work Package (WP5). Decisions regarding access to sensitive data will be made by the relevant data-owning partner, in line with GDPR and project-specific procedures.

3.2.3. Metadata

Metadata associated with publicly available datasets and publications will be made openly available in accordance with Horizon Europe requirements. Where data is deposited in trusted repositories such as Zenodo, metadata will be released under a public domain dedication (CC0 licence), as required by the Grant Agreement. This ensures that metadata can be freely accessed, reused, and harvested by third parties without restrictions.

Metadata records will include sufficient descriptive information to enable users to understand and access the underlying data. This will typically include elements such as title, authors, description, keywords, publication date, licensing conditions, and access rights (e.g. open or restricted access).

Publicly available data will remain accessible for as long as possible through trusted repositories that ensure long-term preservation. In line with Horizon Europe practices, data will be retained for a minimum period of five years after the end of the project, and longer where feasible.

Metadata will be guaranteed to remain available even in cases where the underlying data is no longer accessible (e.g. due to legal, ethical, or confidentiality constraints). This ensures that the existence, context, and conditions of access to the data remain discoverable over time.

Where necessary, documentation will be provided to ensure that users can access, interpret, and reuse the data. This includes descriptions of file formats, methodologies, and data structures.

The project will prioritise the use of widely adopted and non-proprietary file formats (e.g. PDF, CSV) to minimise the need for specialised software. Where specific tools or software are required, this will be clearly documented.

Where explicitly required, relevant software components or scripts may be shared under open-source licences, provided that no legal, security, or confidentiality constraints apply. This will further support transparency, reproducibility, and reuse of project outputs.

3.3. Making data interoperable

The WEM Cyber project will ensure interoperability of data by adopting widely used, non-proprietary formats, general-purpose metadata standards, and established best practices for data management. Given the nature of the project as a Coordination and Support Action, the data generated is primarily related to training, project management, and dissemination, and does not require highly specialised disciplinary standards.

To facilitate data exchange and reuse, the project will use commonly accepted file formats such as PDF, CSV, XLSX, and other interoperable digital formats. Metadata associated with publicly available outputs will follow standard schemas provided by trusted repositories (e.g. Dublin Core via Zenodo), ensuring compatibility with external systems and indexing services.

The project will follow general interoperability best practices promoted by Horizon Europe and OpenAIRE, including the use of structured metadata, clear documentation, and standardised naming conventions. These measures ensure that data can be easily interpreted and reused across different disciplines and organisational contexts.

Where project-specific terminology is used (e.g. in training materials or methodologies), it will be clearly defined and documented to ensure clarity and reuse. If needed, such terminology will be aligned with commonly used concepts in cybersecurity and research policy domains.

Where relevant, data and publications will include references to related datasets, project outputs, or external resources, ensuring contextualisation and facilitating reuse. This includes links between deliverables, training materials, and outputs generated during secondments.

3.4. Increase data re-use

The WEM Cyber project will support data re-use by providing appropriate documentation accompanying all publicly available datasets and outputs. This will include descriptive information on the context of data generation, methodologies applied, and where relevant, explanations of variables, formats, and data structures. Such documentation will typically be provided through repository metadata, accompanying reports, and, where appropriate, readme-style descriptions.

Publicly shareable data and project outputs will be made available in open-access repositories (e.g. Zenodo) to enable the widest possible reuse. In line with Horizon Europe requirements, data will be licensed under standard reuse licences, such as Creative Commons licences (e.g. CC BY), unless restrictions apply due to legal, ethical, or confidentiality considerations.

The project ensures that data remains usable by third parties after the end of the project by relying on trusted repositories that guarantee long-term preservation and access. In addition, the use of widely adopted formats and clear documentation will facilitate interpretation and reuse across different user groups.

Each partner collects their own data, and they are individually responsible for cleaning and classifying it in strict accordance with the GDPR. Following this, BV, as the Lead DPO, conducts



the final GDPR compliance review and enforces the necessary access permissions across the centralized infrastructure.

Data quality will be ensured through internal review and validation processes. Project partners will be responsible for verifying the accuracy, completeness, and consistency of the data they generate. Standardised templates, version control mechanisms, and coordination procedures will further support data quality and integrity throughout the project lifecycle.



**Funded by
the European Union**

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101216854

4. OTHER RESEARCH OUTPUTS

The WEM Cyber project will produce a range of research outputs beyond data, whose management, accessibility, and reuse are described in this chapter.

4.1. Management of research outputs

In addition to research data, the WEM Cyber project will generate a range of research outputs that support its objectives of strengthening cybersecurity capacity, fostering knowledge transfer, and promoting skills development. These outputs are primarily digital in nature and arise from training activities, secondments, mentoring programmes, and dissemination efforts.

The outputs include training and educational materials, methodological frameworks, analytical reports, and policy-oriented documents. Secondment activities may also produce additional outputs such as analyses, technical documentation, or applied methodologies. Furthermore, content and resources will be developed and shared through the Knowledge Transfer Platform, contributing to collaboration and long-term impact.

All research outputs will be managed following the same structured approach as applied to research data. They will be stored in secure and organised environments, primarily within the project's SharePoint infrastructure, and will be subject to version control and internal validation procedures. Each output will be appropriately documented, including information on authorship, date of creation, and its relation to specific work packages or project activities. This ensures traceability, consistency, and transparency across the consortium.

Given the nature of the project, which includes personal data and potentially sensitive cybersecurity-related content, certain outputs may be subject to access restrictions. In such cases, appropriate safeguards will be applied in line with legal, ethical, and contractual requirements, including access control, anonymisation or pseudonymisation, secure storage, encryption where applicable, and the use of contractual measures such as confidentiality agreements.

4.2. Accessibility and sharing

In line with Horizon Europe open science principles, the project will make research outputs openly available wherever possible. Publicly shareable outputs will be disseminated through recognised open-access repositories, such as Zenodo, as well as through the project's Knowledge Transfer Platform and other communication channels.

Where outputs contain personal data, confidential information, or content that may be sensitive from a cybersecurity perspective, access will be restricted and managed through

controlled mechanisms. This ensures compliance with applicable regulations, including GDPR, as well as the protection of the legitimate interests of project partners.

4.3. Application of FAIR principles

Although FAIR principles are primarily defined for research data, they will also be applied, where relevant, to other research outputs generated within the project. Outputs will be described using appropriate metadata, made accessible through recognised platforms, and provided in widely used and interoperable formats.

In addition, sufficient documentation will be provided to enable understanding and reuse of the outputs. This approach supports discoverability, accessibility, and reusability, and ensures that project results can be effectively used by stakeholders beyond the consortium.

4.4. Re-use and long-term availability

The project will take appropriate measures to ensure that research outputs remain available and usable beyond its duration. Public outputs will be deposited in repositories that ensure long-term preservation and accessibility. Where possible, outputs will be made available under standard open licences, such as Creative Commons licences, to facilitate reuse.

Particular attention will be given to the development of training materials and methodologies, ensuring that they are designed for reuse and adaptation in future initiatives. This contributes to the sustainability and long-term impact of the project, especially in the context of capacity building in cybersecurity.

5. ALLOCATION OF RESOURCES

The allocation of resources for managing data and research outputs within the WEM Cyber project, including associated costs, responsibilities, and long-term preservation, is described in this chapter.

5.1. Costs of data and research output management

The WEM Cyber project recognises that the implementation of FAIR principles and the management of research outputs require both direct and indirect resources. These include costs related to data storage, repository use, data curation, documentation, access management, and long-term preservation.

Given the nature of the project as a Coordination and Support Action, the expected costs remain moderate and are primarily associated with the use of existing digital infrastructure and services. These include the use of secure cloud-based collaboration platforms (e.g. SharePoint and Microsoft Teams), as well as open-access repositories (e.g. Zenodo) for the publication and long-term preservation of research outputs.

Additional effort is required for the preparation of metadata, documentation, and quality assurance processes, which are integrated into the day-to-day activities of project partners rather than treated as separate cost items.

5.2. Coverage of costs

All costs related to data and research output management are covered within the overall Horizon Europe project budget, in accordance with the provisions of the Grant Agreement. This includes both direct costs (e.g. personnel time dedicated to data management tasks) and indirect costs (e.g. use of institutional infrastructure and digital services).

The project relies primarily on existing institutional resources and widely available platforms, which ensures cost-efficiency and sustainability. No significant additional financial burden is anticipated beyond standard project management and dissemination activities.

5.3. Responsibilities for data management

Responsibility for data management within the WEM Cyber project is distributed across the consortium in a structured and coordinated manner with clearly defined roles for governance, implementation, and oversight.

The Project Coordinator ensures overall compliance with the Data Management Plan, Horizon Europe requirements, and consortium-level coordination. Work package leaders are responsible for overseeing data management activities within their respective work

packages, including ensuring that data is properly documented, stored, and processed in accordance with this DMP.

Bilişim Vadisi (BV) acts as the Lead Data Protection Officer (Lead DPO) and is responsible for the overall ethical governance of data within the project. This includes leading GDPR compliance activities, coordinating ethical compliance reviews, preparing consent forms, and managing cross-border data transfer mechanisms such as Standard Contractual Clauses (SCCs).

The University of Maribor (UM) provides guidance and validation support to partners. In particular, UM is responsible for developing project-wide guidelines on data handling processes (e.g. anonymisation, pseudonymisation, data minimisation) and for performing a control and double-check mechanism to support compliance. However, responsibility for implementation remains with individual partners.

Individual partners are responsible for the data and research outputs they generate, including ensuring data quality, classification, documentation, and compliance with legal and ethical requirements. Decisions regarding data sharing (open vs restricted) are made by the data-owning partner, in line with project rules and under the oversight of the Lead DPO.

Access to data is granted based on role-based permissions defined by data owners, with oversight from BV as Lead DPO.

Platform-related responsibilities are divided as follows: technical data processing within the Knowledge Transfer Platform is managed by UBITECH, while partners remain responsible for the content they upload.

This distributed model ensures accountability, consistency, and alignment with ethical and legal requirements across all project activities.

5.4. Long-term preservation

The WEM Cyber project will ensure the long-term preservation of relevant data and research outputs through the use of trusted repositories and institutional infrastructures.

Publicly available outputs will be deposited in open-access repositories such as Zenodo, which provide long-term preservation, persistent identifiers, and continued accessibility. Internal and restricted data will be retained within institutional systems for a defined period, in line with legal and contractual obligations.

Data selection for long-term preservation will be based on its relevance, potential for reuse, and compliance with legal and ethical constraints. Priority will be given to publicly shareable outputs such as publications, training materials, and methodologies.



As a general rule, data will be retained for a minimum of five years after the end of the project, unless longer retention is justified or required. Decisions regarding long-term preservation will be made by the relevant data-owning partners, in coordination with the Project Coordinator and in line with project policies.

This approach ensures that the value of project outputs is maintained over time while balancing costs, legal obligations, and practical considerations.



**Funded by
the European Union**

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101216854

6. DATA SECURITY

The measures implemented to ensure the security, integrity, and protection of data within the WEM Cyber project are described in this chapter.

6.1. Data security measures

The WEM Cyber project implements a comprehensive set of technical and organisational measures to ensure the security, integrity, and availability of data throughout its lifecycle. Data security is addressed in a manner proportionate to the nature of the data, with particular attention given to personal data and potentially sensitive cybersecurity-related information.

During the project, data will be stored in secure digital environments, primarily using Microsoft SharePoint, Microsoft Teams, Knowledge Transfer Platform, project website and Sploro platform. These platforms provide controlled access, authentication mechanisms, and built-in security features, including encryption and activity monitoring. Technical security measures such as encryption are implemented at the level of institutional systems and platform providers (e.g. Microsoft services and Sploro), while overall oversight of data protection is ensured by BV as Lead Data Protection Officer.

Access to data is managed through role-based permissions, ensuring that only authorised users can access specific datasets. Additional security procedures include the application of anonymisation and pseudonymisation techniques, whereby personal identifiers are either removed or replaced with coded references to protect the identity of individuals.

Secure data transfer is ensured through the use of encrypted communication protocols (e.g. HTTPS), as well as through the controlled sharing functionalities provided by the project's collaboration tools. Where necessary, additional safeguards will be applied to sensitive data, including anonymisation or pseudonymisation.

Technical security measures such as encryption are implemented at the level of institutional systems and external platforms (e.g. SharePoint, Sploro platform). The Knowledge Transfer Platform, operated by UBITECH, implements its own security architecture, including authenticated user access, secure data storage, and compliance with applicable data processing agreements and data residency requirements. UM provides guidance on data handling and security practices, but does not directly manage or implement encryption mechanisms.

6.2. Data recovery and continuity

To ensure data availability and resilience, appropriate data recovery and backup mechanisms are in place. The cloud-based infrastructure used by the project includes



Funded by
the European Union

automated backup systems and version control, allowing for the recovery of previous versions of documents in case of accidental deletion or data corruption.

These mechanisms ensure continuity of operations and minimise the risk of data loss, contributing to the overall robustness of the data management approach.

6.3. Secure storage and long-term preservation

For long-term preservation, publicly available data and research outputs will be deposited in trusted open-access repositories such as Zenodo. These repositories provide secure storage, persistent identifiers, and long-term curation in accordance with international standards.

Restricted or sensitive data will not be deposited in open repositories. Instead, such data will be stored within secure institutional systems, with access limited to authorised users and retention aligned with legal and contractual requirements.

6.4. Protection of sensitive data

Special consideration is given to the protection of sensitive data, including personal data and data related to cybersecurity activities. Such data will be handled in accordance with the General Data Protection Regulation (GDPR) and relevant ethical guidelines.

Measures include controlled access, data minimisation, and the application of appropriate technical safeguards. The Ethics Work Package (WP5) provides oversight and guidance to ensure that data security practices remain compliant and effective throughout the project.

6.5. Data breach response

In the event of a personal data breach, the project will follow a structured response procedure in line with GDPR requirements.

All partners are required to immediately report any suspected or confirmed data breach to BV, acting as Lead DPO. BV is responsible for assessing the breach, coordinating the response, and determining whether notification to the relevant supervisory authority is required.

Where applicable, BV will ensure that the supervisory authority is notified within 72 hours of becoming aware of the breach, in accordance with GDPR Article 33. If the breach is likely to result in a high risk to data subjects, affected individuals will also be informed without undue delay.

UM supports this process by providing guidance and validation where necessary, while partners are responsible for initial detection and reporting.

This procedure ensures a coordinated, timely, and compliant response to data security incidents.

6.6.Data retention

Personal data will be retained only for as long as necessary to fulfil the purposes of the project, in accordance with the storage limitation principle of GDPR. In general, personal data will be retained for a maximum of 5 years after the end of the project, unless longer retention is required by legal or contractual obligations.

Non-personal research data and publicly available outputs will be preserved for the long term through trusted repositories (e.g. Zenodo) to ensure continued accessibility and reuse.



**Funded by
the European Union**

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101216854

7. ETHICS

The ethical and legal considerations relevant to data handling within the WEM Cyber project, including compliance with data protection regulations, are described in this chapter.

7.1. Ethical and legal considerations

The WEM Cyber project recognises that ethical and legal considerations are central to data management, particularly in the processing of personal data for training, mentoring, coaching and secondment activities.

The primary legal framework governing data protection within the project is the General Data Protection Regulation (GDPR). All personal data will be processed in accordance with GDPR principles, including lawfulness, fairness, transparency, data minimisation, purpose limitation, and confidentiality.

Ethical governance within the project is led by BV, acting as Lead Data Protection Officer (Lead DPO). BV is responsible for coordinating ethical compliance reviews, ensuring alignment with GDPR requirements, and overseeing the implementation of safeguards across all Work Packages. UM supports this process by providing guidance, validation, and control mechanisms.

Ethics monitoring will be implemented through structured procedures developed within WP5. This includes a task-based ethics monitoring checklist applied during project activities, as well as a secondment ethics pre-checklist that must be completed prior to the start of secondment processes. These checks are integrated into existing project review and validation workflows to ensure continuous compliance.

Given the involvement of a non-EU partner (Türkiye), personal data may be transferred outside the European Economic Area in the context of secondment activities. Such transfers will be carried out in full compliance with GDPR requirements, using appropriate safeguards such as Standard Contractual Clauses (SCCs) [4]. BV is responsible for the preparation and implementation of SCCs, while UM provides advisory and reminder support. SCCs apply specifically to personal data transfers, while non-personal data transfers are governed by contractual and organisational arrangements within the consortium. All transfers will be limited to the minimum necessary data and conducted within secure environments.

Ethical aspects related to data management are addressed within the framework of the project's Ethics Work Package (WP5) and are aligned with the ethics requirements described in the Description of the Action (DoA). Ethical compliance is implemented as a continuous process throughout the project and includes the application of GDPR principles,



Funded by
the European Union

the maintenance of records of processing activities, and the application of data protection safeguards.

As defined in this DMP, WP5 establishes practical procedures for ethical governance, including the use of ethics monitoring checklists, secondment pre-assessment procedures, informed consent management, and oversight of cross-border data transfers. These procedures complement the compliance measures described in the DoA and ensure consistent implementation across all project activities.

7.2. Informed consent

Informed consent procedures will be implemented for all activities involving the collection and processing of personal data. Participants will be clearly informed about the purpose of data collection, the types of data processed, their rights under GDPR, and the conditions for data storage, sharing, and reuse.

WPI facilitates the coordination of inputs from data-generating work packages (WP2, WP3, and WP4) and supports the harmonisation of consent form templates across the consortium, ensuring consistency in data protection practices across different project activities.

Consent forms will be developed and maintained by BV in its role as Lead DPO. UM will support the process by performing a review and double-check mechanism to ensure completeness and compliance. Final approval of all consent forms rests with the Lead DPO (BV), under the governance of WP5.

Consent forms will explicitly include information on:

- data sharing within the consortium,
- long-term storage and retention,
- potential use of anonymised or aggregated data for research and dissemination purposes,
- cross-border data transfers where applicable.

Participation will be voluntary, and participants will have the right to withdraw their consent at any time, without negative consequences, in accordance with GDPR requirements.

7.3. Artificial intelligence and data use

Some project activities may involve the use of artificial intelligence technologies, particularly in the context of cybersecurity research and training. The use of third-party AI tools (e.g. external cloud-based services) is restricted to non-sensitive and non-personal data unless appropriate data processing agreements are in place. Project partners are not permitted

to submit personal or restricted project data to external AI systems without prior assessment and approval. AI-generated outputs will be reviewed by project partners before being incorporated into deliverables.

In such cases, all data used for AI-related activities will be handled in accordance with applicable legal and ethical requirements. In cases where AI-related activities involve personal data, processing will only take place based on a valid legal basis, including informed consent where applicable. Particular attention will be given to:

- avoiding the use of personal data unless strictly necessary,
- ensuring data quality and representativeness,
- mitigating potential bias in datasets and outputs,
- maintaining transparency in methodologies where relevant.

AI-related activities will follow the same standards of data protection, security, and ethical compliance as all other project activities. This integrated approach ensures that ethical and data protection requirements are consistently applied across all project activities.



**Funded by
the European Union**

8. OTHER ISSUES

The WEM Cyber project primarily follows the data management requirements and principles established under Horizon Europe, including compliance with the FAIR principles and the provisions set out in the Grant Agreement.

In addition, the project benefits from and aligns with existing institutional and organisational data management procedures of the participating partners. These include internal policies and practices related to data protection, information security, and research data management, implemented at the university and industry partners levels.

As defined in this DMP, these procedures cover aspects such as secure data storage, access control, data retention, and compliance with legal frameworks, including the General Data Protection Regulation (GDPR). The use of established institutional infrastructures, such as secure cloud-based systems and repository services, further supports the implementation of these practices.

The project does not rely on specific sectorial or national data management frameworks beyond those already embedded within partner institutions. However, all partners are expected to ensure that their internal procedures are consistent with Horizon Europe requirements and the provisions of this Data Management Plan.



Funded by
the European Union

CONCLUSION

This Data Management Plan provides a comprehensive and structured framework for the management of data and other research outputs within the WEM Cyber project. It ensures full alignment with Horizon Europe requirements and demonstrates a strong commitment to the FAIR principles, open science practices, and responsible data management.

The project adopts a pragmatic and proportionate approach, balancing the objective of making data and outputs as openly available as possible with the need to protect personal data, confidential information, and potentially sensitive cybersecurity-related content. Through the use of trusted repositories, standardised formats, and clear documentation, the project ensures that its outputs are accessible, reusable, and valuable to a wide range of stakeholders.

At the same time, robust data security measures, GDPR compliance, and ethical oversight mechanisms are in place to ensure that data is handled responsibly throughout its lifecycle. The involvement of a non-EU partner is addressed through appropriate safeguards for international data transfers, ensuring continued compliance with European data protection standards.

The DMP also recognises the importance of managing research outputs beyond data, ensuring that training materials, methodologies, and best practices are preserved and made available for future use, thereby contributing to the long-term impact and sustainability of the project.

As a living document, this Data Management Plan will be reviewed and updated throughout the project to reflect evolving needs, risks, and best practices, ensuring that data management remains effective, compliant, and aligned with the project's objectives.



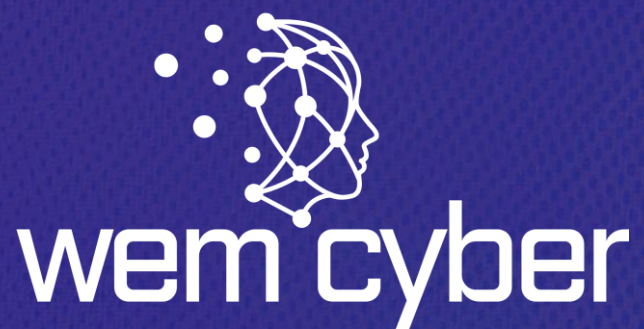
Funded by
the European Union

REFERENCES

- [1] M. D. Wilkinson *et al.*, "The FAIR Guiding Principles for scientific data management and stewardship," (in En), *Scientific Data*, BriefCommunication vol. 3, no. 1, p. 160018, 2016–03–15 2016, doi: doi:10.1038/sdata.2016.18.
- [2] "Zenodo." @zenodo_org. <https://about.zenodo.org/> (accessed 31 March, 2026).
- [3] "General Data Protection Regulation (GDPR) – Legal Text." <https://gdpr-info.eu/> (accessed 31 March, 2026).
- [4] "Standard Contractual Clauses (SCC)." https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en (accessed 31 March, 2026).



Funded by
the European Union



Consortium



Funded by
the European Union