Cynergy4ME

Chips JU

Funded by the European Union

Bridging Ecosystems for European Technological Advancement

Deliverable	**Data Management Plan**		
Deliverable File	D8.2		
Project	Cynergy4MIE	**Grant Agreement Number**	101140226
Lead Beneficiary	AVL	**Dissemination Level**	Public
Involved SC's	All partners	**Related Task/s**	T8.1, T8.2
Due Date	M6	**Actual Submission Date**	M8
Status	Final	**Version**	1.0
Contact Person	Katrin Al Jezany, Manuel Staud	**Organisation**	AVL List GmbH
Phone	+43 664 2892612	**E-Mail**	katrin.aljezany@avl.com manuel.staud@avl.com

Document history			
V	**Date**	**Author**	**Description**
0.1	30.01.2025	Manuel Staud	Draft Chapters proposal
0.2	25.03.2025	Christina Vrotsou	Finalised draft of chapter 11
0.3	11.04.2025	Manuel Staud	First reviewed version
1.0	29.04.2025	Manuel Staud	Final and reviewed Version

Acknowledgement

CYNERGY4MIE receives funding within the Key Digital Technologies Joint Undertaking (KDT JU) - the Public-Private Partnership for research, development and innovation under Horizon Europe – and National Authorities under Grant Agreement No 101140226.

Table of contents

1 List of Abbreviations and Acronyms

Table 1 summarizes the abbreviations and acronyms used in this document.

TABLE 1: ACRONYMS & ABBREVIATIONS

Abbreviation/Acronym	Meaning
DMP	Data Management Plan
CA	Consortium Agreement
GA	Grant Agreement
LM	Liaison Manager
DPO	Data Protection Officer
WP	Work Package
SC	Supply Chain
FAIR	Findable, Accessible, Interoperable and Reusable
GDPR	General Data Protection Regulation
EU	European Union
EA	Ethics Advisor
PC	Project Coordinator
DPIA	Data Protection Impact Assessment
SCC	Standard Contractual Clause
DPA	Data Processing Agreement

2 Executive summary

The Data Management Plan (DMP) provides guidance and best practice for data management within the Cynergy4MIE project.

The Data Management Plan (DMP) focuses on these three main tasks:

1. Protect commercially sensitive data.
2. Publication and Dissemination of project findings wherever possible.
3. Compliance with GDPR and/or other relevant personal data laws and requirements.

2.1 DMP execution & target groups

The execution of the Data Management Plan is the responsibility of all project members - relative to their roles and responsibilities. The Project Coordinator (PC), Work Package (WP) leaders, Supply Chain (SC) leaders and Task leaders, will provide wide reaching project support to implement the Data Management Plan and provide additional support where required.

The DMP describes the FAIR - Findable, Accessible, Interoperable and Reusable - best practice for data management (please see Section 7 for details on FAIR.)

The DMP provides guidance on how to label and classify data as well as the processes through which partners should go before making any data publicly available. This includes guidance on how to identify who is responsible for a data set, along with respective roles and responsibilities of project members relative to their ownership of or usage of data.

This Data Management Plan (DMP) defines procedures on how to handle personal data to guarantee project participants' fundamental rights and avoid misuse of the project results. The DMP complies with EU and international regulations for the management and use of data and will pay particular attention to the General Data Protection Regulation (GDPR), which came into effect in 2018.

If you are, or think you maybe, dealing with personally identifiable data you will be classed as a 'data controller' under GDPR. Whenever any project member intends on collecting, processing, or using personally identifiable data of any kind, GDPR and other legal compliance requirements must first be considered.

This DMP provides:

- **The key definitions**
- **The key principals**
- **Accessing further guidance**

As soon as partners are aware that data and findings are of public value, they will begin, in accordance with the guidance in this Data Management Plan - and the terms of the CA and GA - exploring the possibility of making that data publicly accessible. The DMP provides best practice guidance and processes for making data available within the project and in order that that data be maintained and available beyond the time frame of the project.

Moreover, the DMP recommends approaches to data security and storage. Finally, the DMP gives recommendations on whether data will be destroyed at the end of the project or archived for further use by the research community. In the latter case, the DMP provides recommendations for future maintenance and access to the data by consortium partners and external parties.

However, it should be noted that the DMP is in no way a substitute for the projects legal documents and do not replace their enforcement in any way – if in doubt the legally binding documentation takes precedence.

3 Non-Publishable Information

Not applicable.

4 Contribution of Partners

The Cynergy4MIE DMP profited from the contributions of multiple partners, please see Table 2.

TABLE 2: CONTRIBUTION OF CYNERGY4MIE PARTNERS TO THIS DATA MANAGEMENT PLAN

Chapter	Partner	Contribution
All	AVL	Draft preparation
All	AVL	Adjustments do draft
All	AVL	Chapters adaption
All	AVL	Chapters: insert contents
11	CONV	Provision of contents
All	GRO	Review of contents

5 Introduction & Scope

5.1 Purpose

The Cynergy4MIE Data Management Plan (DMP) is thought to be a document that outlines the strategies and procedures for managing research data. It serves as a roadmap, providing guidance on how data will be collected, organized, stored, shared, and preserved. The DMP promotes transparency, efficiency, and compliance with data management best practices and funder requirements.

The purpose of a DMP is to ensure effective management of data to maximize its value and accessibility. The DMP helps to better understand data organization, data documentation, data security, data sharing and dissemination, and long-term data retention. This minimizes potential problems, enables data integrity and improves the overall quality and impact of Cynergy4MIE research activities.

The Data Management Plan (DMP):

I) **Outlines the data management procedures and infrastructure** that will be used, including data collection methods, data storage and backup systems, metadata standards, and data security measures.

II) **Includes a description of the research project and the types of data that will be generated or collected.**

III) **Addresses data sharing and access policies, specifying who will have access to the data, under what conditions, and for how long.**

IV) **Describes any restrictions on data sharing due to privacy concerns, confidentiality requirements, intellectual property rights, or legal and ethical considerations.**

V) **Additionally covers plans for long-term data preservation**, including strategies for data archiving, metadata preservation, and data format migration to ensure data longevity and accessibility.

In summary, the Data Management Plan outlines the strategies and procedures for managing research data throughout its lifecycle. It promotes good data management practices, facilitates data sharing and preservation, and enhances the overall integrity and impact of Cynergy4MIE research.

5.2 Target group

The execution of the Data Management Plan is the responsibility of all project members - relative to their roles and responsibilities. The Project Coordinator (PC), Work Package (WP) leaders, Supply Chain (SC) leaders and Task leaders, will provide wide reaching project support to implement the Data Management Plan and provide additional support where required.

Data generated in Cynergy4MIE will be stored in different locations based on its accessibility. The consortium defines four levels:

- **Partner**: accessible only by the partner that generates it.
- **Parts of Consortium**: E.g. Supply Chain or Task

- **Consortium**: data generated by a single partner (or multiple partners) that should be accessible to all partners.
- **Public**: data generated by a partner (or multiple partners) that is accessible to the public.

5.3 Cynergy4MIE guiding principles

Cynergy4MIE follows the FAIR data access according to the principle *<<as open as possible, as closed as necessary>>* Practical guide to address Open Science issues in Horizon Europe[1] (Figure 1):

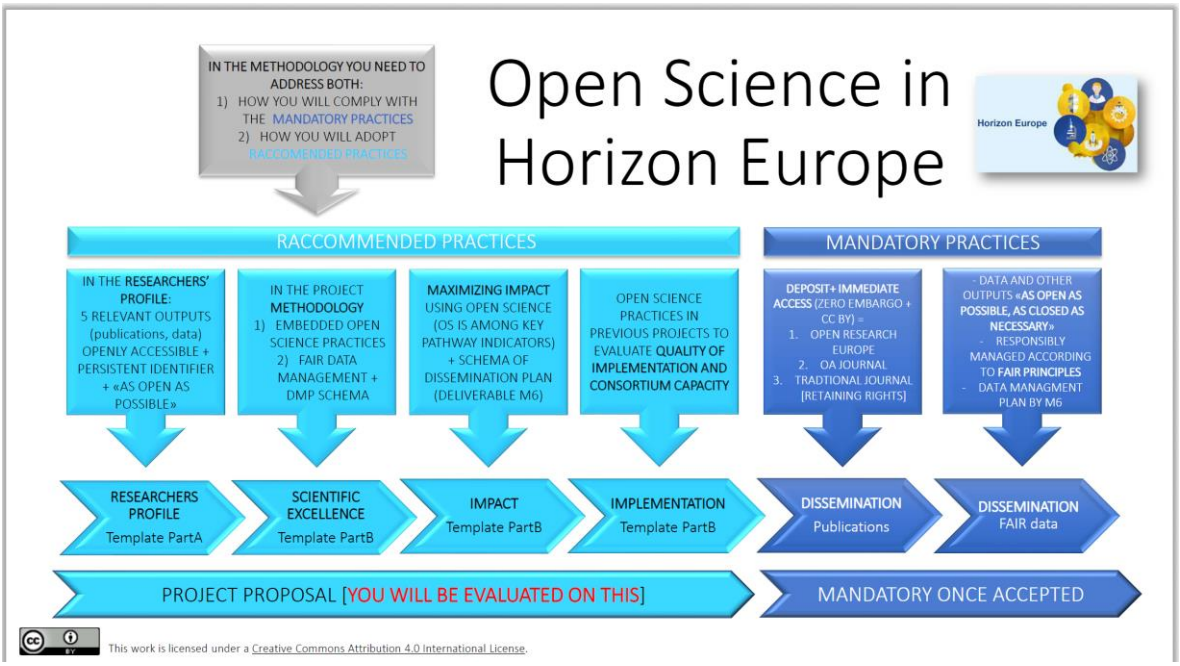

FIGURE 1: OPEN SCIENCE IN THE RECOMMENDED AND MANDATORY PRACTICES.

To comply with the open science nature of HE researches, open access data with dissemination purposes will be stored in one of these two widely accepted general purpose repositories:

Zenodo[2]: it is a CERN datacenter-backed research data repository for the long-tail of science, enabling researchers to preserve and share their research output from any science, regardless of the size and format. ZENODO is an innovative and easy to use web-platform, which allows uploading, curating and sharing of the research data through an easy-to-use web interface and integration with other collaboration and data sharing services. ZENODO ensures the discovery and citability of the research output by assigning a Digital Object Identifier (DOI) to every upload, as well as promotes software citation and preservation through one-click integration with GitHub. For all public open data, it will remain reusable via Zenodo for at least 20 years (as stated by the Zenodo Repository).

[1] *Practical guide to address Open Science issues in Horizon Europe: mandatory and recommended Open Science practices, intellectual property rights and Open practices, rights retention clause to deposit and give immediate access…*

The infographic has been adapted from https://osf.io/dp6je/ created by the Open science team, Ghent University Library.

[2] https://zenodo.org/

Open Research Europe[3]: "*is an open access publishing platform for the publication of research stemming from Horizon 2020, Horizon Europe and/or Euratom funding across all subject areas. The platform makes it easy for Horizon 2020, Horizon Europe and Euratom beneficiaries to comply with the open access terms of their funding and offers researchers a publishing venue to share their results and insights rapidly and facilitate open, constructive research discussion.*

While open access to research data thereby becomes applicable by default in Horizon 2020, the Commission also recognizes that there are good reasons to keep some or even all research data generated in a project closed.

The Commission therefore provides robust opt-out possibilities at any stage, that is during the application phase during the grant agreement preparation (GAP) phase and after the signature of the grant agreement.

The ORD pilot applies primarily to the data needed to validate the results presented in scientific publications. Other data can also be provided by the beneficiaries on a voluntary basis, as stated in their Data Management Plans. Costs associated with open access to research data, can be claimed as eligible costs of any Horizon 2020 grant."

[3] https://open-research-europe.ec.europa.eu/

"Participating in the ORD Pilot does not necessarily mean opening up all your research data. Rather, the ORD pilot follows the principle "as open as possible, as closed as necessary" and focuses on encouraging sound data management as an essential part of research best practice.[4]"

Best efforts will be made to integrate all content into suitable alternative institutional and/or subject based repositories.

5.4 Data inventory for information collection

The data inventory table is a document or Excel File used to collect and organize information about the data assets within the Cynergy4MIE project. It serves as a centralized repository for collecting the details about each dataset, facilitating efficient data management, and providing a comprehensive overview of the available data resources (Table 3).

TABLE 3: DATA INVENTORY

Data Code	Data Name	Data type	Open / Restricted	Data utility	Data creation via	Size	Stored in	Who can use the data	Ethical issues yes/no

5.5 Dissemination data groups

PUBLIC DELIVERABLES

[4] https://ec.europa.eu/research/participants/docs/h2020-funding-guide/cross-cutting-issues/open-access-data-management/data-management_en.htm

Dx,y TITLE Description and relation to the DMP.

TITLE	*Lead Beneficiary*	*WP*	*Type*	*Dissemination*
D1.1 TITLE	XXX	WP1	DMP	PU

5.6 Open access

The Cynergy4MIE consortium is informed about the obligation (GA, article 17) to ensure open access to peer-reviewed scientific publications relating to their results.

They must ensure that:

- at the latest at the time of publication, a machine-readable electronic copy of the published version or the final peer-reviewed manuscript accepted for publication, is deposited in a trusted repository for scientific publications
- immediate open access is provided to the deposited publication via the repository, under the latest available version of the Creative Commons Attribution International Public Licence (CC BY) or a licence with equivalent rights; for monographs and other long-text formats, the licence may exclude commercial uses and derivative works (e.g. CC BY-NC, CC BY-ND)information is given via the repository about any research output or any other tools and instruments needed to validate the conclusions of the scientific publication.

Beneficiaries (or authors) must retain sufficient intellectual property rights to comply with the open access requirements. Metadata of deposited publications must be open under a Creative Common Public Domain Dedication (CC 0) or equivalent, in line with the FAIR principles (in particular machine actionable) and provide information at least about the following: publication (author(s), title, date of publication, publication venue); Horizon Europe or Euratom funding; grant project name, acronym and number; licensing terms; persistent identifiers for the publication, the authors involved in the action and, if possible, for their organizations and the grant. Where applicable, the metadata must include persistent identifiers for any research output, or any other tools and instruments needed to validate the conclusions of the publication. Only publication fees in full open access venues for peer-reviewed scientific publications are eligible for reimbursement.

The approach of the consortium to open science follows “The Guidelines on Open Access to Scientific Publications and Research Data” in Horizon Europe and aligns a strategy for knowledge management and protection to enable broader, faster, more transparent and equal access for the benefit of researchers, industry and citizens. The project partners are committed to provide open-access to all peer-reviewed publications relating to the results of the project. This will be achieved either via green

(self-archiving) or via gold open access (author-pays-model). During the proposal preparation phase, the consortium reviewed the key open-access policies of relevant publishers in our field (including IEEE, ACM, Springer, and Elsevier) and budgeted reasonable publication costs to allow for open access publishing via the gold open access, also known as the "author pays-model"). The consortium will also base its green open access of the project publications on the infrastructure of the EU project OpenAIRE. The OpenAIRE's catch-all data repository Zenodo is publicly available for all researchers and is designed to measure compliance with the EC's Open Access policies and pilots. The OpenAIRE-compliant repository Zenodo is hosted by CERN that uses self-developed software to host and store data and publications produced within different kinds of projects. Software tools developed by the consortium will be released with open-source licenses according to relevance and market potential to generate versatile solutions. Some of the background tools and libraries already use such open-source license, e.g. RTAMT is licensed under BSD 3-clause. This policy enables the scientific community to benefit from our results and continue research and improving the tools for wider use than done in this project. Software results will be distributed using traditional channels such as Gitlab and major Linux distribution repositories when they can be considered stable.

5.6.1 Process for the dissemination approval

Following the Project Consortium Agreement requirements, during the Cynergy4MIE project and for a period of 1 year after the end of the project, the Dissemination of own Results by one or several Parties including but not restricted to publications and presentations, shall be governed by the procedure of Article 17.4 of the Grant Agreement and its Annex 5, Section Dissemination, subject to the following provisions.

A beneficiary that intends to disseminate its results must give at least 15 days advance notice to the other beneficiaries (unless agreed otherwise), together with sufficient information on the results it will disseminate.

Any other beneficiary may object within (unless agreed otherwise) 15 days of receiving notification, if it can show that its legitimate interests in relation to the results or background would be significantly harmed. In such cases, the results may not be disseminated unless appropriate steps are taken to safeguard those interests.

An objection is justified if

a) the protection of the objecting Party's Results or Background would be adversely affected, or

b) the objecting Party's Legitimate Interests would be significantly harmed, or

c) the proposed publication includes Confidential Information of the objecting Party.

The objection has to include a precise request for necessary modifications.

If an objection has been raised the involved Parties shall discuss how to overcome the justified grounds for the objection on a timely basis (for example by amendment to the planned publication and/or by protecting information before publication) and the objecting Party shall not unreasonably continue the opposition if appropriate measures are taken following the discussion.

The objecting Party can request a publication delay of not more than 60 calendar days from the time it raises such an objection. After 60 calendar days the publication is permitted, provided that the objections of the objecting Party have been addressed.

A Party shall not include in any Dissemination activity another Party's Results, Background or Confidential Information even if such Results, Background or Confidential Information is amalgamated with Party´s Results without obtaining the owning Party's prior written approval.

The Parties undertake to cooperate to allow the timely submission, examination, publication and defense of any dissertation or thesis for a degree that includes their Results, Background or Confidential Information subject to the confidentiality and publication provisions agreed in this Consortium Agreement. The disclosure of Confidential Information to the student's supervisor and supervising university not being part of the Consortium for the purpose of the respective supervision is permitted on a need to know basis as long as they are bound by a confidentiality obligation no less stringent than the terms and conditions as provided in Section 10.

In the frame of Cynergy4MIE project, the processes of dissemination approval are managed by dissemination Partner TeraGlobus (TG), monitoring the prior notifications about the upcoming dissemination cases. Each partner in the consortium handles their publications on the F&T portal. TG handles other dissemination cases' listing and delivering to related deliverables and F&T portal.

6 Cynergy4MIE Project Summary

Cynergy4MIE aims to advance technologies in Mobility, Infrastructure, and Energy (MIE) by creating a unified technology stack. This will facilitate the seamless transfer of smart software and efficient electronic components, accelerating product development and reducing costs. The project addresses global challenges like climate change, energy economy, and affordability by focusing on software-driven approaches and shared tools, particularly for electric vehicles and energy storage solutions.

Key innovations include minimally invasive sensors for electric drives, smart battery packs with distributed learning and quantum sensors, and methodologies for optimized traffic flow using V2X communication. Additionally, Cynergy4MIE will develop AI/ML algorithms for search and rescue missions using UAV and UGV platforms equipped with specialized sensors.

The project aims to converge the MIE ecosystems towards a de-carbonized, digitalized, and green EU, building trust in new technologies and contributing to the affordability of energy and goods while ensuring a safe and secure society.

6.1 Objectives

The project aims to revolutionize various aspects of Cyber-Physical Systems (CPS) through five key objectives shown in Figure 2.

FIGURE 2: CYNERGY4MIE - OBJECTIVES

Objective 1 focuses on designing and deploying minimally invasive sensors for critical nano/microstructures. By leveraging advanced quantum and mm-wave sensors, the goal is to enable multi-modal measurements and enhance the capabilities of CPS in challenging environments.

Objective 2 aims to integrate built-in AI for coexistence and collaboration within CPS, particularly in safety-critical contexts. This involves enhancing human-machine collaboration, ensuring secure and reliable AI-driven systems, and advancing edge AI, human-robot interaction, and safety verification.

Objective 3 is dedicated to building digital assets and emergent AI to improve operational efficiency. This includes developing AI-driven platforms that facilitate collaboration among multi-robot systems, particularly for tasks such as search and rescue, thereby boosting efficiency and reliability.

Objective 4 seeks to accelerate convergence in ecosystems to achieve economies of scale. By optimizing CPS to enhance energy and resource efficiency, the project aims to drive innovation, create new business opportunities, and foster economic growth through the integration of mobility, infrastructure, and energy systems.

Objective 5 focuses on enhancing global competitiveness for Europe’s circular economy. This involves applying circular economy principles to promote sustainable industrial production, improve resource efficiency, and strengthen the EU's position in the global market.

6.2 Project partners

Cynergy4MIE brings together expertise from about 43 partners out of 16 countries, see Figure 3.

FIGURE 3: CYNERGY4MIE CONSORTIUM AND COUNTRY COVERAGE

A full list of the Cynergy4MIE Participants is shown in Table 4.

TABLE 4: LIST OF CYNERGY4MIE PARTICIPANTS

Part. No.	*Participant organisation name*	*Participant short name*	*Type*	*Role*	Country	National eligibility checked by participant (Y/N)
1	AVL LIST GMBH	AVL	LE	CO	AT	Y
2	SILICON AUSTRIA LABS GMBH	SAL	RES	BEN	AT	Y
3	INFINEON TECHNOLOGIES AUSTRIA AG	IFAT	LE	BEN	AT	Y
4	VIRTUAL VEHICLE RESEARCH GMBH	VIF	RES	BEN	AT	Y
5	VYSOKE UCENI TECHNICKE V BRNE	BUT	RES	BEN	CZ	Y
6	TECHNISCHE UNIVERSITAET GRAZ	TUG	RES	BEN	AT	Y
7	IDEAS & MOTION SRL	I&M	SME	BEN	IT	Y
8	VERUM SOFTWARE TOOLS B.V.	VER	SME	BEN	NL	Y

9	TEKNOLOGIAN TUTKIMUSKESKUS VTT OY	VTT	RES	BEN	FI	Y
10	TECHNISCHE HOCHSCHULE ROSENHEIM / TECHNICAL UNIVERSITY OF APPLIED SCIENCES	THRO	RES	BEN	DE	Y
11	ELEKTRONIKAS UN DATORZINATNU INSTITUTS	EDI	RES	BEN	LV	Y
12	GIM OY	GIM	SME	BEN	FI	Y
13	SYGKLISI ASTIKI MI KERDOSKOPIKI ETAIREIA	CONV	RES	BEN	GR	Y
14	IOTAM INTERNET OF THINGS APPLICATIONS AND MULTI LAYER DEVELOPMENT LTD	IOTAM	SME	BEN	CY	Y
15	NXP SEMICONDUCTORS NETHERLANDS BV	NXP-NL	LE	BEN	NL	Y
16	VAISTO SOLUTIONS OY	VAISTO	SME	BEN	FI	Y
17	ZF FRIEDRICHSHAFEN AG	ZF	LE	BEN	DE	Y
18	INSAR.SK SRO	INSAR	SME	BEN	SK	Y
19	XENOMATIX	XENOMATIX	SME	BEN	BE	Y
20	SMARTSOL SIA	SSOL	SME	BEN	LV	Y
21	INSTITUT MIKROELEKTRONICKYCH APLIKACI SRO	IMA	LE	BEN	CZ	Y
22	FRAUNHOFER GESELLSCHAFT ZUR FORDERUNG DER ANGEWANDTEN FORSCHUNG EV	Fraunhofer	RES	BEN	DE	Y
23	PRODRIVE TECHNOLOGIES INNOVATION SERVICES B.V.	PRODRIVE	LE	BEN	NL	Y
24	UNIVERSITAET GRAZ	KFU	RES	BEN	AT	Y
25	DRIVEU TECH LTD	DRIVEU	SME	BEN	IL	Y
26	TECHNISCHE UNIVERSITEIT EINDHOVEN	TU/e	RES	BEN	NL	Y
27	STMICROELECTRONICS SRL	ST-I	LE	BEN	IT	Y

28	TECHNISCHE UNIVERSITEIT DELFT	TUD	RES	BEN	NL	Y
29	GROPYUS TECHNOLOGIES GMBH	GRO	SME	BEN	DE	Y
30	KUNGLIGA TEKNISKA HOEGSKOLAN	KTH	RES	BEN	SE	Y
31	STRIKERSOFT AB	STRIKERSOFT	LE	BEN	SE	Y
32	MURATA ELECTRONICS OY	MURATA	LE	BEN	FI	Y
33	MEDISYS MONOPROSOPI IKE	MEDISYS	SME	BEN	GR	Y
34	TTTECH AUTO AG	TAAT	LE	BEN	AT	Y
35	POLITECNICO DI TORINO	POLITO	RES	BEN	IT	Y
36	SLEEP ADVICE TECHNOLOGIES SRL	SAT	SME	BEN	IT	Y
37	MEVEA OY	MEV	SME	BEN	FI	Y
38	UAB TERAGLOBUS	TG	SME	BEN	LT	Y
39	INDUSTRIAL TECHNOLOGY RESEARCH INSTITUTE INCORPORATED	ITRI	RES	AssoPart	TW	Y
40	BOARD OF REGENTS OF NEVADA SYSTEM OF HIGHER EDUCATION	UNEV	RES	AssoPart	US	Y
41	FRIEDRICH-ALEXANDER-UNIVERSITAET ERLANGEN-NUERNBERG	FAU	RES	AssoPart	DE	Y
42	RECHI PRECISION CO.,LTD	RECHI	LE	AssoPart	TW	Y
43	FUTU-RE Co., Ltd.	FUTURE	LE	AssoPart	JP	Y

6.3 Cynergy4MIE supply chains & work packages

The work plan has been designed according to the widely adopted V-cycle model, cf. Figure 4. After working out detailed requirements and specifications as well as systems architectures and models in WPs 1 and 2, the main research and implementation work is conducted in WPs 3 and 4 before an integration phase in WP5 and the final validation and verification actions in WP6 are conducted. In parallel and over the whole duration of the project, WPs 7 and 8 cover dissemination, exploitation, communication, standardization, and project management respectively.

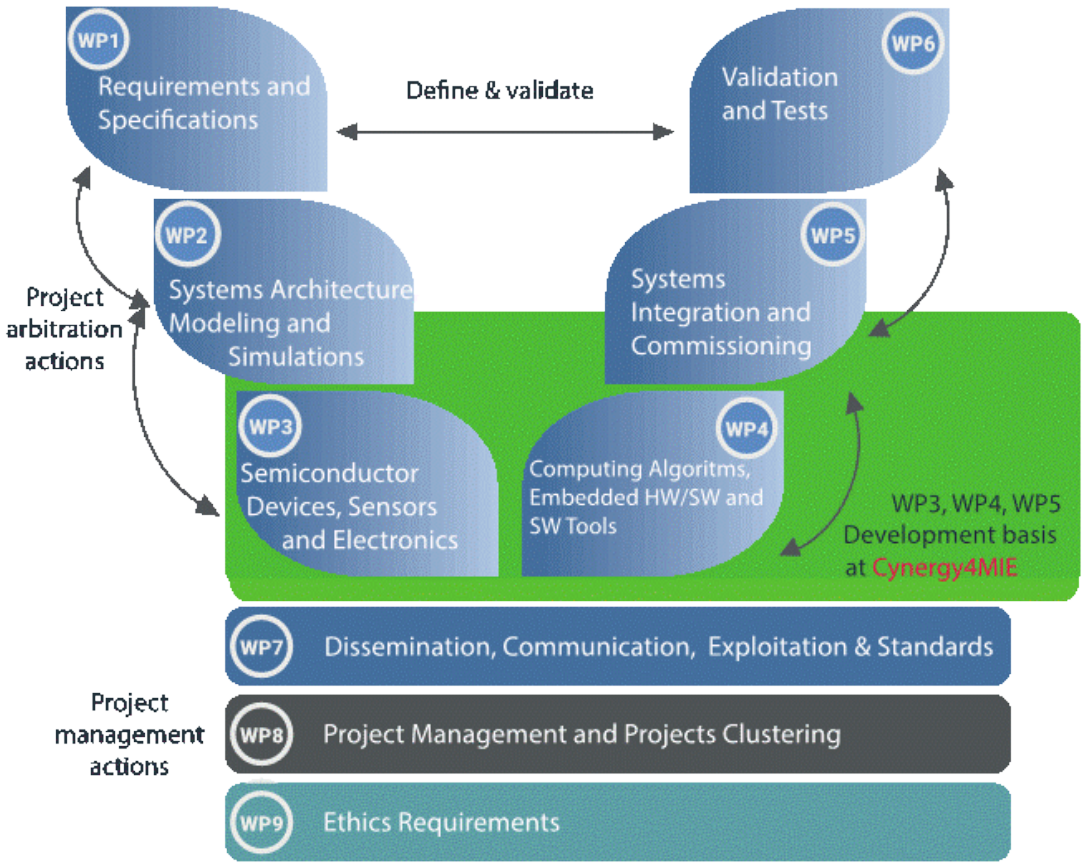

FIGURE 4: CYNERGY4MIE WORK-PACKAGE STRUCTURE

Besides WPs, ***Cynergy4MIE*** is also structured into SCs, yielding the matrix organization as shown in Figure 5. The idea of SCs is to group research activities around common topics. Put differently, each SC concentrates on the development of one sub-topic addressed by ***Cynergy4MIE***. For doing so, each SC defines specific tasks in WPs of ***Cynergy4MIE***. These tasks will be worked off according to the V-cycle model referred to above. This setup allows "locked, stepwise execution" between SCs and, hence, cross SC synchronization in each phase, e.g., when elaborating requirements or validating the project results with respect to the requirements and KPIs. At the same time, SCs improve the manageability of ***Cynergy4MIE*** as there are defined leaders for each sub-topic, that would not be available in a WP-only structure. Every SC starts with the definition of specifications and requirements derived from the project key targets with respect to the defined KPIs. Next, new technology is researched/developed based on these specifications and requirements. After the development and integration, the integrated (sub) systems are tested to verify their functionalities, and their behavior/performance is compared/validated according to the original specification and requirements. The benefits of this approach were already proved in previous projects, e.g., 3Ccar, AutoDrive, NewControl, AI4CSM or A-IQ Ready.

Cynergy4MIE comprises 6 SCs dedicated to several automotive and industrial applications of emergent systems based on novel semiconductors solutions.

A careful partitioning of work and the definition of clear interfaces between the different Work Packages (WPs) and SCs is required for the success of the ***Cynergy4MIE*** project. As discussed, the

Cynergy4MIE project will provide an approach where WPs represent the R&D domains with a focus on technologies and methodology, while SCs (described in Section 1) represent real implementation, demonstrators, experimental work, and implementation efforts leading to the integration of the (sub)systems and their verification and validation. The relation of the SCs and the WPs is depicted in Figure 5, whereas the interrelation of the ***Cynergy4MIE*** WPs is shown in Figure 6.

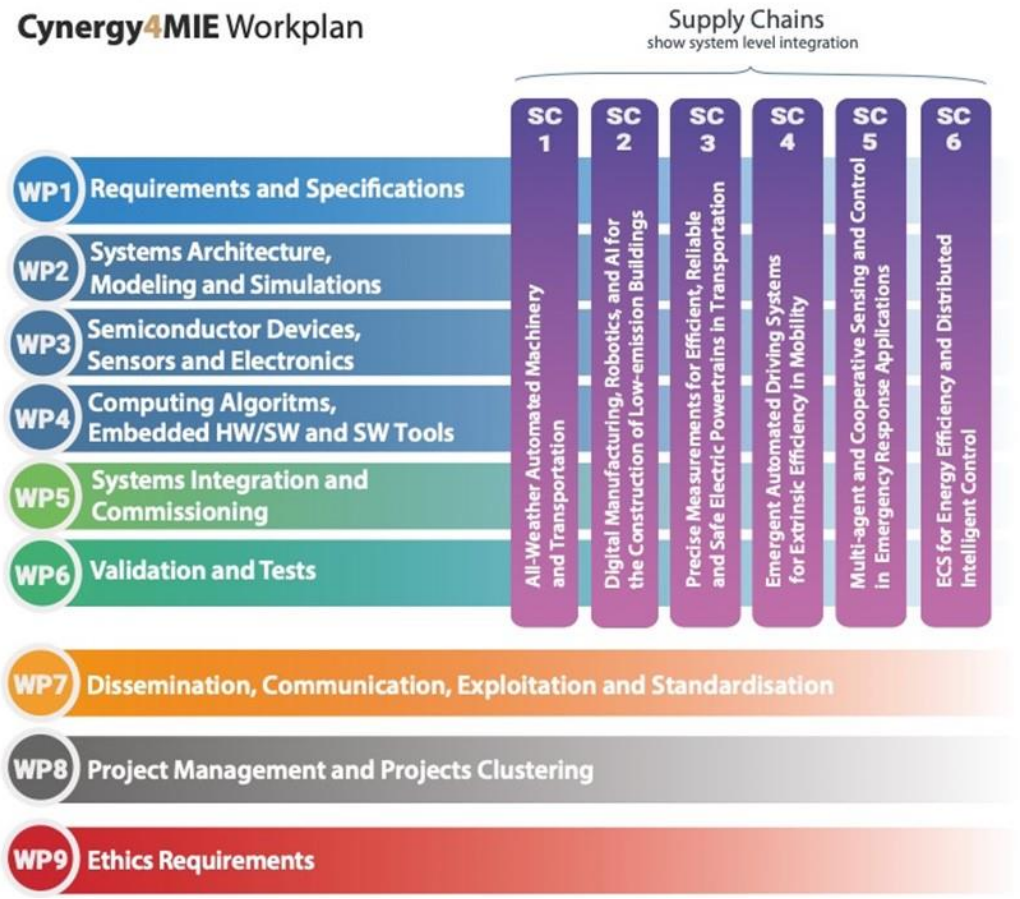

FIGURE 5: CYNERGY4MIE MATRIX STRUCTURE OF WPS AND SCS

WP1 defines the system requirements as well as the use cases and validation methodologies, also making sure research results of ***Cynergy4MIE*** are aligned with targets set by the Green Deal, Ethics guidelines, and relevant upcoming standards. WP2 is dedicated to analysis and definition of emergent systems architecture as well as their modelling and simulation to obtain early knowledge on systems behavior necessary for individual HW and SW development steps. WP3 is dedicated to development and manufacturing of new components, including novel quantum sensors and related electronic circuits for sensing, signals processing and power-electronics. WP4 will evaluate and design computing platforms and embedded HW/SW necessary for individual SCs. WP4 also includes development and implementation of embedded AI to support emergent behavior of systems in individual SCs as well as other algorithms to be implemented in embedded SW covering control, diagnostics, and fault mitigation in emergent systems as well as qualification related topics linked specially to stress conditions specific for automotive and industrial applications.

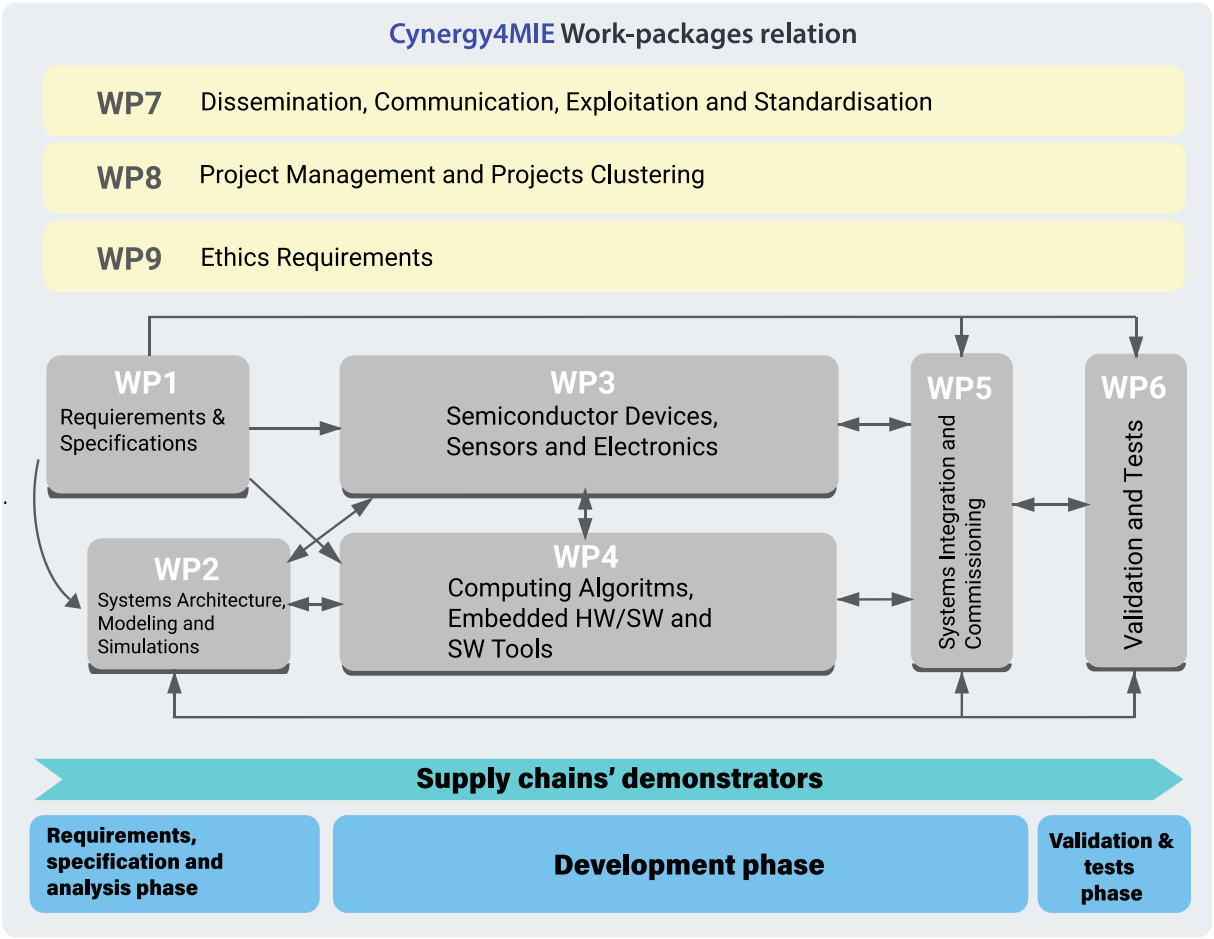

FIGURE 6: CYNERGY4MIE WORK PACKAGE RELATIONS

WP5 cares about the system integration for each supply chain. Outcome of WP5 will be set of commissioned demonstrators ready for in-depth testing. Within the frame of WP6, validation and testing of the SC demonstrators takes place. It focuses on behavior validation of the developed subsystems with the goal to demonstrate the properties, safety, flexibility, and performance of the developed solutions in relation to the requirements defined in WP1. WP7 covers exploitation, dissemination, communication, standardization, and also market trends monitoring to analyze the solutions developed by competitors. WP8 performs the overall project management, including monitoring and all financial & contractual aspects.

The project will benefit from a bi-directional flow of information between work-packages. Research running in a given work-package will use outputs supplied by earlier work-packages (stages of the V-cycle), but also provide feedback to these WPs, to correct possible problems in the designed solutions. For example, WP4 will respond to feedback from WP5 and WP6 to resolve possible problems during system integration and testing by smart SW solutions. The timing of the WPs contains significant time overlap of WPs with strong interrelations to allow efficient bidirectional flow of information and iterative development process as mentioned bellow.

In more detail, WP1 provides requirements and specifications for the analysis and design of architectures performed by WP2, and the development phase covered WP3 and WP4. These WPs also provide feedback to WP1 if some requirements or specifications need to be refined or extended. WP2 supports the development of components and HW/SW in WP3 and WP4 as well as initial steps of

subsystems and systems integration in WP5 with knowledge of emergent systems behavior obtained from simulations. WP5 integrates the components, electronics and computing HW/SW provided by WP3 and WP4 and uses knowledge of simulations outcomes from to build emergent subsystems and systems. In the case of unexpected problems with integration and commissioning of the subsystems and systems, feedback to WP3 and WP4 will allow the change of component designs to solve possible problems. Finally, the subsystems and systems are tested and validated in WP6 where conformance with specifications from WP1 will be checked.

7 FAIR Data Management

FAIR data refers to a set of principles aimed at enhancing the accessibility and usability of research data. The acronym "FAIR" stands for Findable, Accessible, Interoperable, and Reusable, highlighting key aspects that contribute to the overall quality and value of research data [5].

Findable: data should be easily discoverable and identifiable using unique identifiers, metadata, and standardized descriptions. This enables researchers, and interested parties, to locate and access the data efficiently.

Accessible: data should be openly available or accessible with clear and defined protocols, allowing users to retrieve and obtain the data without unnecessary barriers or restrictions. Access should be granted based on appropriate permissions and data usage agreements.

Interoperable: data should be structured and formatted in a way that facilitates seamless integration and interoperability with other datasets. Commonly accepted standards and protocols should be followed to ensure compatibility and the ability to combine data from various sources.

Reusable: data should be well-documented, clearly described, and include sufficient contextual information to enable its reuse for different purposes. This includes providing information on the methodology, data collection procedures, and any applicable licensing or usage terms.

By adhering to the FAIR data principles, researchers and organizations can enhance the value and impact of their data, promote collaboration and knowledge exchange, and facilitate the reproducibility of research. FAIR data principles are becoming increasingly important in the scientific community as they contribute to transparency, data sharing, and the advancement of research across disciplines.

More detailed information will be included in the questionnaire (Appendix 1) to which each partner will answer. This file will be part of the final report as part of the dissemination, exploitation, and data management of the project.

The exchange of data and information within the project is crucial for the success of the technological development and achievement of the project objectives. In this way, the data flow between the different SCs and WPs is essential. Figure 7 below shows the plan of data flow between SCs and WPs. The technical development of the project demonstrators and their use cases is performed in the SCs. The specified tasks in the technical WPs are responsible for keeping track of important data that is generated by the SCs within a specific point in technology development. Finally, any specific data and information that is required for project management, i.e. project risk mitigation or reporting, is shared with the Project Coordinator within WP8, and any data or information that is required for project outreach, dissemination, exploitation and publications is shared by the SCs and WPs to the WP7.

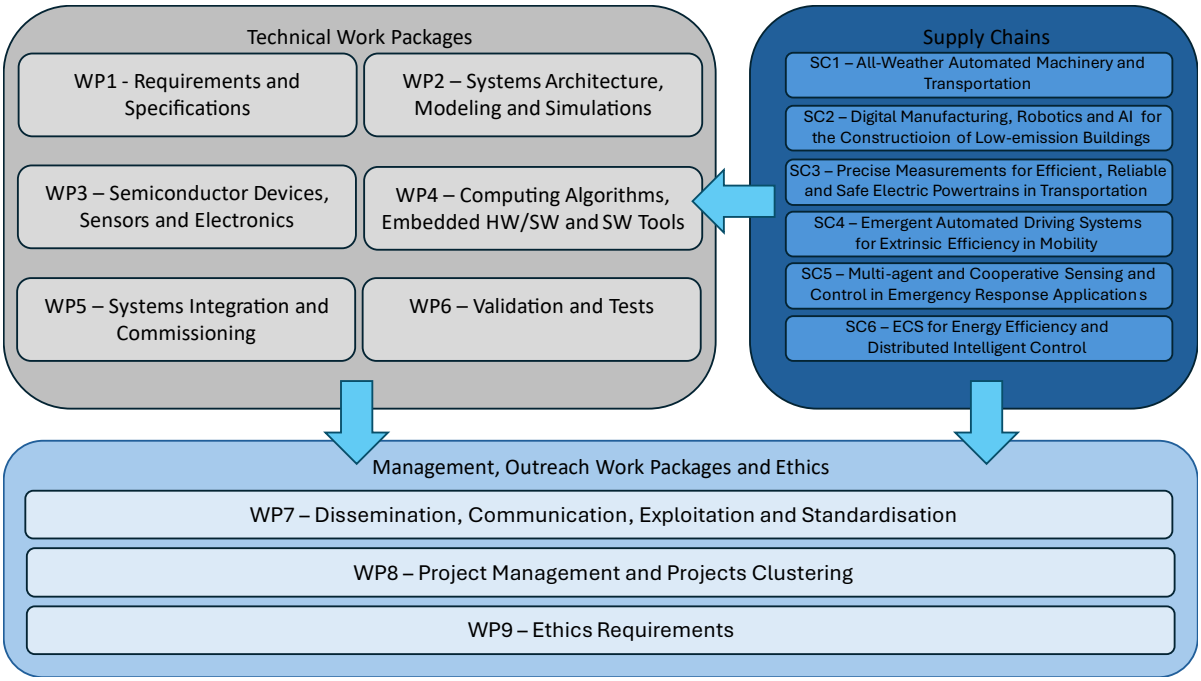

FIGURE 7: INFORMATION AND DATA FLOW IN CYNERGY4MIE

7.1 Making data findable, including provision of metadata

Data generated in Cynergy4MIE will be stored in different locations based on its accessibility.

The consortium defines four levels:

- **Partner:** accessible only by the partner that generates it
- **Parts of Consortium:** E.g. Supply Chain or Task
- **Consortium:** data generated by a single partner (or multiple partners) that should be accessible to all partners
- **Public:** data generated by a partner (or multiple partners) that is accessible to the public

7.1.1 Default catalogue metadata schema for open data generated by the project

Knowledge workers spend more than 50% of their time looking for information; it is a fundamental aspect to improve their experience by providing quick access to resources they need during and after the duration of the project. Classification and implementation of content metadata play a crucial role in that manner.

Metadata is the data that describes other data. It is essential to identify, locate and describe digital objectives generated by Cynergy4MIE, such as videos, files, images, websites, etc. They are helpful to assist users in finding and organizing the information generated.

In general the ZENODO repository metadata domain presented in Section 5.3 is based on DataCite's metadata that you find in the link: https://schema.datacite.org/meta/kernel-4.4/doc/DataCite-MetadataKernel_v4.4.pdf (Version 2021) with the title **"Metadata Schema Documentation for the Publication and Citation of Research Data and Other Research Output"**[5].

[5] https://schema.datacite.org/meta/kernel-4.4/doc/DataCite-MetadataKernel_v4.4.pdf
https://schema.datacite.org/meta/kernel-4.4/

This document underlines the minimum recommended metadata schema terms should be used for open data generated by a project and deposited in an open access repository. The motivation is underlined by this explanation:

"Scholarly research is producing ever-increasing amounts of digital research data, and it depends on data to verify research findings, create new research, and share findings. In this context, what has been missing until recently is a persistent approach to access, identification, sharing, and re-use of datasets.

To address this need, the DataCite[6] international consortium was founded in late 2009 with these three fundamental goals:

- establish easier access to scientific research data on the Internet,
- increase acceptance of research data as legitimate, citable contributions to the scientific record,
- support data archiving that will permit results to be verified and re-purposed for future study."

Below you find the Mandatory and the Recommended and Operational properties suggested. For Definitions and Allowed values, examples or other constraints we remand to the link above.

TABLE 5 DATACITE MANDATORY PROPERTIES ARE:

ID	Property	Obligation
1	Identifier (with mandatory type sub-property)	M
2	Creator (with optional given name, family name, name identifier and affiliation sub-properties)	M
3	Title (with optional type sub-properties)	M
4	Publisher	M
5	PublicationYear	M
10	ResourceType (with mandatory general type description subproperty	M

TABLE 6 DATACITE RECOMMENDED AND OPERATIONAL PROPERTIES:

ID	Property	Obligation
6	Subject (with scheme sub-property)	R
7	Contributor (with optional given name, family name, name identifier, and affiliation sub-properties)	R
8	Date (with type sub-property)	R

[6] https://datacite.org/

9	Language	O
11	AlternateIdentifier (with type sub-property)	O
12	RelatedIdentifier (with type and relation type sub-properties)	R
13	Size	O
14	Format	O
15	Version	O
16	Rights	O
17	Description (with type sub-property)	R
18	GeoLocation (with point, box, place, and polygon sub-properties)	R
19	FundingReference (with name, identifier, and award related subproperties	O
20	RelatedItem (with identifier, creator, title, publication year, volume, issue, number, page, publisher, edition, and contributor sub-properties)	O

7.1.2 How will the data be openly accessible in the project

Data generated in Cynergy4MIE will be stored in different locations based on its accessibility. The consortium defines four levels:

- **Partner**: accessible only by the partner that generates it.
- **Parts of the Consortium:** accessible to partners working together on technology development
- **Consortium**: data generated by a single partner (or multiple partners) that should be accessible to all partners.
- **Public**: data generated by a partner (or multiple partners) that is accessible to the public.

In the Cynergy4MIE Data Management Plan, Section "Data Storage, Access & Security", Question 29 "*If you have answered yes to the previous question, please specify which data will be made open access."* addresses open accessible data that concerns the Cynergy4MIE project, please see Figure 8.

FIGURE 8: WORD CLOUD EVALUATION OF CYNERGY4MIE DMP QUESTIONNAIRE – QUESTION 29.

7.1.2.1 *Open Data for publication*

Communities: List of communities the deposition to appears in ***Collection***

URL:

https://zenodo.org/communities/Cynergy4MIE/

Above address links directly to your community collection.

Upload URL:

https://zenodo.org/deposit/new?c=Cynergy4MIE

Above address will automatically ensure people who use it will have their record added to your community collection.

A Decision Diagram of the "Research to Publication – Process" is shown in Figure 9.

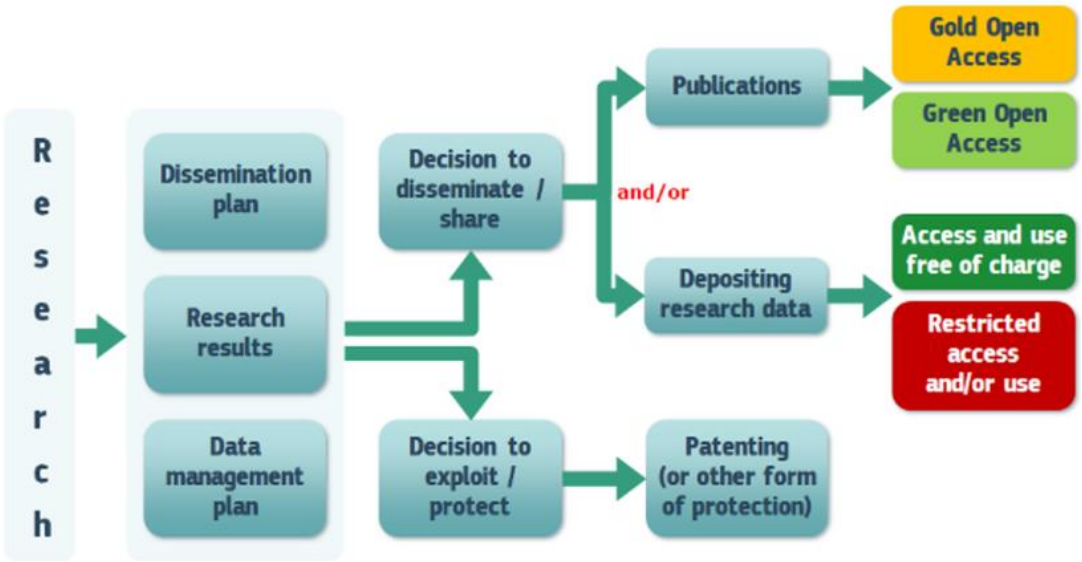

FIGURE 9: OPEN ACCESS TO RESEARCH AND PUBLICATION DECISION DIAGRAM [7].

7.1.2.2 Scientific Publications

The Consortium will fully address the European Commission requirements through the support of open access for published articles. Scientific publications of project's results will be granted open access according to publisher and law regulations as set out in the Grant Agreement. Depending on the nature of the publication, the articles will be made available immediately through open access publishing ('gold' open access) (e.g., by an open access journal) or within a period of 6 months through self-archiving ('green' open access). *Cynergy4MIE* partners have already established various Open Access policies: supporting authors in retaining their rights to provide access to published articles, providing official repositories, and making the bibliographic metadata that identify the deposited publication available to OpenAIRE[24].

Other means include finding suitable repositories via OpenAIRE, the Registry of Open Access Repositories[25], and the Directory of Open Access Repositories[26]. Furthermore, all published scientific publications will be accessible on the Cynergy4MIE website. *Cynergy4MIE* aims to engage with multiple stakeholders and develop an open-source information ecosystem with tools and knowledge available to all.

7.1.2.3 Green open access (self-archiving)

Green open access or self-archiving means that the published article or the final peer-reviewed manuscript is archived by the researcher itself in an online repository, in most cases after its publication in the journal. The journal must grant the researcher the permission to self-archive the final peer-reviewed article, at the latest, 12 months after publication.

7.1.2.4 Gold open access (open access publishing)

Gold open access means that the publication is available by the scientific publisher as open access. Some journals require an author-processing fee for publishing open access. Author-publishing fees for gold open access journals can be reimbursed within the project period and budget. Some publishers allow the researcher to deposit a copy of the article in a repository, sometimes with an embargo period.

8 Personal Data and GDPR

The Cynergy4MIE project will comply with GDPR and/ or other relevant personal data laws and requirements. The PCA (4.5) states:

Where necessary, the Parties shall cooperate in order to enable one another to fulfil legal obligations arising under applicable data protection laws (*the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and relevant national data protection law applicable to said Party*) within the scope of the performance and administration of the Project and of this Consortium Agreement.
In particular, the Parties shall, where necessary, conclude a separate data processing, data sharing and/or joint controller agreement before any data processing or data sharing takes place.

In case an additional agreement related to the processing of personal data is deemed necessary according to the Applicable Laws, or desirable by Parties, the Parties shall enter into good faith negotiations to reach such an agreement.
In particular, the Parties shall, where necessary, conclude a separate data transfer, data processing, data sharing and/or joint controller agreement before any data processing or data sharing takes place.

As part of compiling this Data Management Plan, all project participants were asked to complete the Cynergy4MIE Data Management Questionnaire. Please see Section 14 for details. The questionnaire has provided valuable insight to the data types the project forecasts to generate.

Personally identifiable data could be very simple (i.e. a list of project contacts) or detailed and extensive (i.e. a systematic interview study with many stakeholders).

Any project member intending to collect, process, or use personally identifiable data of any kind must first consider GDPR and other legal compliance requirements. Below an overview of GDPR considerations are provided, together with a set of further resources and support that can be accessed to help in final decision making.

8.1 Key definitions

The GDPR defines an array of legal terms at length. Below are some of the most important ones (https://gdpr.eu/what-is-gdpr/):

- **Personal data:** Personal data is any information that relates to an individual who can be directly or indirectly identified. Names and email addresses are obviously personal data. Location information, ethnicity, gender, biometric data, religious beliefs, web cookies, and political opinions can also be personal data. Pseudonymous data can also fall under the definition if it's relatively easy to ID someone from it.
- **Data processing**: Any action performed on data, whether automated or manual. The examples cited in the text include collecting, recording, organizing, structuring, storing, using, erasing…
- **Data subject**: The person whose data is processed. These are your customers or site visitors.
- **Data controller:** The person who decides why and how personal data will be processed. If you're an owner or employee in your organization who handles data, this is you.

- **Data processor:** A third party that processes personal data on behalf of a data controller. The GDPR has special rules for these individuals and organizations. They could include cloud servers or email service providers.

Please note that the Data Controller of any individual data set that requires GDPR consideration is the one responsible for ensuring GDPR obligations are accurately covered.

8.2 Key principals

If you process data, you must do so according to seven protection and accountability principles (https://gdpr.eu/what-is-gdpr/):

- **Lawfulness, fairness and transparency** — Processing must be lawful, fair, and transparent to the data subject. One of the following 6 must apply (Art. 6 GDPR - Lawfulness of processing - GDPR.eu):
    1. Consent provided.
    2. Performance of a contract.
    3. Compliance with a legal obligation.
    4. Protection of the vital interests of the data subject.
    5. Performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
    6. Legitimate interests pursued by the controller or by a third party.
- **Purpose limitation** — You must process data for the legitimate purposes specified explicitly to the data subject when you collected it.
- **Data minimization** — You should collect and process only as much data as absolutely necessary for the purposes specified.
- **Accuracy** — You must keep personal data accurate and up to date.
- **Storage limitation** — You may only store personally identifying data for as long as necessary for the specified purpose.
- **Integrity and confidentiality** — Processing must be done in such a way as to ensure appropriate security, integrity, and confidentiality (e.g. by using encryption). Please see also Section 10 of this DMP for more details.
- **Accountability** — The data controller is responsible for being able to demonstrate GDPR compliance with all these principles.

Please note that a key responsibility of the 'Data Controller' is to document the GDPR decision making processes relating to their data set.

8.3 Accessing further guidance

If you are, or think you maybe, dealing with personally identifiable data you will be classed as a 'data controller'. To ensure GDPR compliance the following steps are recommended:

1. Consult with your organisational GDPR expert and other available organisational material.

2. Consult relevant guidance material, such as GDPR.eu (and ico.org.uk in the UK).
3. GDPR.eu provides an accessible check list (GDPR compliance checklist - GDPR.eu) that will help establish the correct processes and procedures in managing personal data.
4. Consult with the Cynergy4MIE project consortium; with the primary contact being the Project lead (please see also Section 7).
5. Record and document your decision making.

9 Open Data

The Cynergy4MIE consortium is committed to providing benefit to the European Community in terms of open and fair access to scientific knowledge, standardization, and economic impact.

Through its dissemination plan the project will aim to make findings and data known and available to specific stakeholders such as industry, policy makers, and standardization bodies. Furthermore, industry associations, stakeholder workshops and wider communications channels will be leveraged to enhance the project outcomes.

Within all these domains the data made available will adhere to certain standards and principles. This will ensure the data meets the FAIR standards of being findable, accessible, interoperable, and reusable (please see also Section 7 – for more information on FAIR). This is not only critical for its use by the intended target stakeholder groups, but also so a wider set of stakeholders from academic, industry and policy have the potential of making use of the data.

The guidelines the project will follow are detailed below (GA, Annex 5):

- Produce a data management plan (DMP) – this document
- Follow the FAIR principals – 'please see Section: 7 of this DMP
- All the relevant peer-reviewed publications relating to the project results will be made available to the Open Research Europe (ORE) (EC's open access publishing platform: https://open-research-europe.ec.europa.eu/).
- A machine-readable electronic copy of the published version or the final peer-reviewed manuscript accepted for publication, is deposited in a trusted repository for scientific publications (at the latest at the time of publication).
- Immediate open access is provided to the deposited publication via the repository, under the latest available version of the Creative Commons Attribution International Public Licence (CC BY) or a licence with equivalent rights; for monographs and other Long-text formats, the licence may exclude commercial uses and derivative works (e.g.CC BY-NC, CC BY-ND)
- Information is given via the repository about any research output, or any other tools and instruments needed to validate the conclusions of the scientific publication. Beneficiaries (or authors) must retain sufficient intellectual property rights to comply with the open access requirements.
- Metadata of deposited publications must be open under a Creative Common Public Domain. Dedication (CC 0) or equivalent, in line with the FAIR principles (in particular machine-actionable) and provide information at least about the following: publication (author(s), title, date of publication, publication venue); Horizon Europe or Euratom funding; grant project name, acronym and number; licensing terms; persistent identifiers for the publication, the authors involved in the action and, if possible, for their organisations and the grant. Where applicable, the metadata must include persistent identifiers for any research output, or any other tools and instruments needed to validate the conclusions of the publication.

As soon as partners are aware data and findings are of public value they will begin, in accordance with the guidance in this plan and the terms of the PCA and GA, exploring the possibility of making that data public. In some instances, the time required to making data available, could be subject to external influences i.e. internal Governance processes or Peer Review. Data will be made available 'as soon as feasible' (GA, Annex 5).

10 Data Storage & Security

10.1 Best practice

The Cynergy4MIE project is forecast to use several data depositories. A secure file sharing and working area for the project partners will be established for the day-to-day operations. However as bespoke software, data and systems are used and generated (i.e. simulation platforms, scenarios, test data) a wider set of depositaries are expected to be used. In all instances project partners will follow the following best practice in selecting, implementing and maintaining data storage facilities:

- **Access Control**: Cynergy4MIE dataset repository must be capable of controlling the level of access that each user has depending on their role. There must be appropriate mechanisms to define and enforce such access control (e.g., firewalls, file systems permissions, secure log-in, password renewal) including physical control. This is provided by the IT department of the repository maintainer or by the dataset repository technology itself.
- **Authentication**: It must guarantee that the system being accessed is the intended one and that the user is who he or she claims to be. During the project, the partners will have access using a private password. Once the datasets become public, an e-mail-based authentication mechanism will grant access.
- **Non-Repudiation**: To ensure the capability to prevent users from denying that data files were accessed, altered, or deleted, auditing processes must be implemented. This is provided by the IT department of the repository maintainer or by the dataset repository technology itself.
- **Data Confidentiality**: Within the scope of the project, the protection of information from unauthorized access and disclosure must be preserved by restricting per-user access and encrypting the information during transmission and also during storage. After the defined retention period expires, information erasure or destruction must be ensured. This is provided by the IT department of the repository maintainer or by the dataset repository technology itself.
- **Communication Security**: Communication only flows through encrypted communication channels. This is provided by the IT department of the repository maintainer or by the dataset repository technology itself.
- **Data Integrity**: Cynergy4MIE must protect data from unauthorized, uncontrolled, or accidental alteration during storage or transmission with the use of checksum values, hash functions and digital signatures. This is provided by the IT department of the repository maintainer or by the dataset repository technology itself.
- **Availability:** Back-up mechanisms are a desirable property, mainly to avoid Denial of Service (DoS) attacks. This is provided by the IT department of the dataset maintainer or by the dataset repository technology itself.

The Cynergy4MIE project has implemented a shared repository for information and documents. This shared repository uses the BOX service, and it is protected by usernames and passwords so that only members that have been granted permission can access it.

The questions 19 and 20 in the Cynergy4MIE DMP Questionnaire ("*Will the data be safely stored in trusted repositories for long term preservation and curation?"* and "Where will this data be stored?") address the topic of safe data storage in the Cynergy4MIE project. The answers are evaluated using pie charts, see Figure 10.

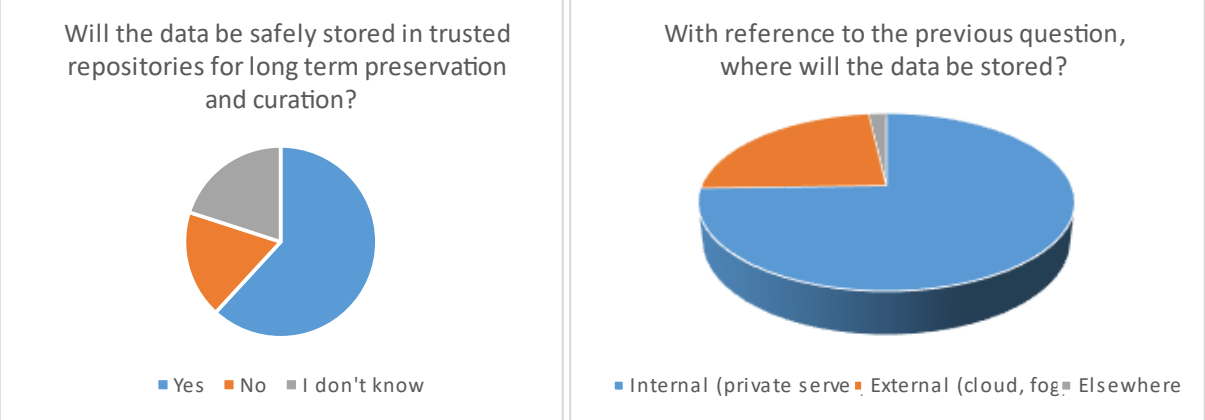

FIGURE 10: DATA STORAGE IN THE CYNERGY4MIE PROJECT.

10.2 Data legacy

Before the end of the Cynergy4MIE project the dissemination and communications activities will establish a legacy plan for the project's outcomes. It is expected that this will include data sets that will be of value to the consortium and wider eco-system beyond the life of the project. For this long-term preservation and curation of data, before the end of the project, an appropriate data repository (or repositories) will be identified and used. Established protocols for making such data sets available for public use such as ZENODO or OpenAIRE with guidelines on how to select such repositories, will be followed. For more information on ZENODO or Open Research Europe, please see Section 5.3 of this data management plan.

The answers to question 10 of the Cynergy4MIE Questionnaire *"What is the expected size of the data that you intend to generate or re-use? (If not a precise figure at least an order of magnitude)"* give an estimate of the data generated by various project partners within the Cynergy4MIE project. Please see Figure 11 for a depiction in a pie chart (the answers were assigned to data intervals).

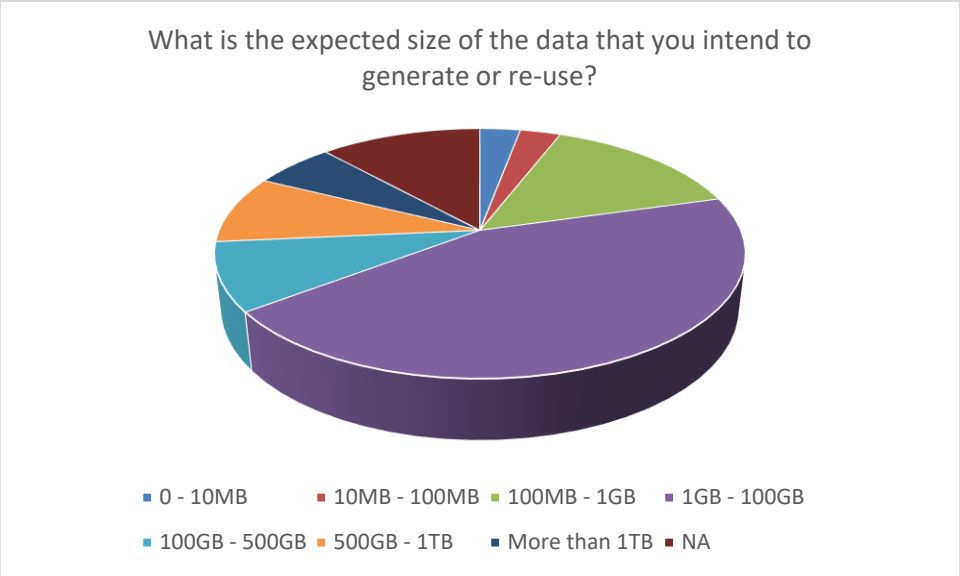

FIGURE 11: SIZE OF GENERATED DATA DURING THE CYNERGY4MIE PROJECT (ESTIMATION).

11 Ethics in Cynergy4MIE

This section outlines the ethical regulations, principles, and compliance measures essential to the Cynergy4MIE project's alignment with EU standards. Ethical compliance is a fundamental requirement for all EU-funded projects, ensuring that research and development activities protect the rights, dignity, and welfare of participants and adhere to the highest standards of transparency and integrity. Ethical considerations also play a fundamental role in Cynergy4MIE's data management practices, ensuring compliance with legal, regulatory, and ethical standards applicable to Horizon Europe projects.

The designated Ethics Work Package for Cynergy4MIE is "WP9- Ethics Requirements" which includes 4 relevant deliverables scheduled for submission in M3, M12, M24 and M36. For D9.1 - EPQ - POPD - NEC - H - AI – Requirement No. 1"[1], submitted M3, it was decided to act proactively and go beyond merely outlining the role and justification of the Ethics Advisor (EA). This deliverable serves as a general guideline for all project partners, outlining the project's comprehensive ethics framework. In particular, D9.1 establishes the following:

- **The regulatory framework for ethical compliance**
  - Regulation 2021/695
  - The European Code of Conduct for Research Integrity
  - EC's guidance on how to complete your ethics self-assessment
- **Key ethical principles and considerations**
  - The principle of proportionality
  - The principle of non-discrimination, inclusivity and fairness
  - Vulnerable subjects
  - The right to the protection of personal data
  - The right to privacy and confidentiality
  - The right to integrity
  - Potential misuse of research findings for unethical purposes
  - Incidental findings in research
- The foundational **ethics framework and monitoring plan for Cynergy4MIE**
  - Guiding ethical principles
  - Procedures for human participation
  - Activities involving non-EU countries
  - Artificial Intelligence (AI) deployment and safety
  - Environmental Health and Safety (EHS) applications
- Formalised the **role of the Ethics Advisor (EA)**
  - Offer guidance to the beneficiary on effectively addressing ethical issues, with the ultimate goal of ensuring the beneficiary's or consortium's compliance with ethical standards.
  - Ongoing ethics monitoring and reporting, documentation of compliance measures, and prompt addressing of any ethics issues that arise
  - Provides independent, impartial guidance on ethical matters but is not legally accountable for non-compliance by partners
  - Acts as an impartial mediator and advisor, reporting unresolved issues directly to the EC if required.
- The requirement for all consortium partners to review D9.1 and sign a letter of intent (LOI) to confirm their commitment to the ethical protocol outlined.
- Furthermore, it includes several **key templates**

- A standardised **informed consent form with a participant information sheet** (Annex A):
  - This template ensures all partners obtain consent in a consistent, GDPR-compliant manner, and it is meant to be adapted to each specific research activity.
- **Risk assessment templates** for activities in both non-EU countries (Annex B) and EU countries (Annex C):
  - These templates guide partners to systematically identify and mitigate safety, legal, and ethical risks for any project tasks outside the EU or within the EU, respectively.
- **Ethics issue reporting and assessment template** (Annex C) for internal ethics monitoring:
  - This reporting template allows partners to document any potential ethics issue encountered during the project and submit it to the Ethics Advisor (EA) and Project Coordinator for review and guidance.

For further details on the project's ethical framework, the reader can refer to D9.1, which presently remains the primary document governing ethics compliance.

11.1 Ethics Considerations in Data Management

This DMP's Ethics section builds upon D9.1 by focusing on data-specific ethical procedures. This section has been drafted upon reviewing responses of the Cynergy4MIE consortium to the DMP questionnaire. The DMP questionnaire includes ethics related questions to assist in the ethics monitoring procedure. As such the purpose here is to underline and briefly describe important procedures relevant for Cynergy4MIE and to evaluate potential ethical issues which may arise so that the EA and PC will be able to follow up and provide guidance as necessary, this last part is outside the scope of this deliverable and solely relates to WP9 activities and respective deliverables.

11.1.1 Conditions where a Data Protection Officer (DPO) is Required

In D9.1, the EA initially recommended appointing a DPO for Cynergy4MIE as a proactive measure intended to strengthen data protection processes and provide a clear point of contact for GDPR compliance questions and potential incidents. However, after reviewing the responses from the DMP questionnaire and subsequent discussions between the EA and PC, it was concluded that a dedicated consortium-level DPO is not necessary at this stage.

To clarify the legal context and individual obligations of partners: under GDPR Article 37, a DPO must be appointed by a controller or processor if any of the following conditions apply: the entity is a public authority or body, or its core activities involve large-scale processing of sensitive data or regular, systematic monitoring of individuals on a large scale [2].

In the context of Cynergy4MIE, the project itself is a consortium of many independent organisations rather than a single legal entity. The project's core objective is technological research (AI, sensors, CPS systems), not the large-scale monitoring or profiling of people, nor the large-scale use of special-category personal data. Personal data processing in the project is incidental and limited to specific use-cases, rather than a core, pervasive activity across the consortium. Therefore, GDPR does not require a dedicated project-level DPO for the consortium as a whole, since the consortium isn't a unified controller with qualifying activities under Article 37 .

Nevertheless, this section clearly underlines that each partner organisation remains individually responsible for fulfilling GDPR compliance obligations, including DPO appointment, as relevant.

11.2 Key Data Management Practices

To align with GDPR and Horizon Europe guidelines, Cynergy4MIE implements data management practices that adhere to strict ethical principles. Building on the previous sections of this deliverable, all partners processing personal data must ensure full compliance with GDPR (Regulation (EU) 2016/679). The following measures apply:

1. Data Protection Impact Assessments (DPIAs): Required for high-risk processing in accordance with Article 35 GDPR[3]
2. Data Processing Agreements (DPAs): Mandatory under Article 28 GDPR where a partner processes personal data on behalf of another[4]
3. Standard Contractual Clauses (SCCs): Required under Article 46 GDPR[5] for international data transfers to countries without an EU adequacy decision
4. Data minimisation and security: Personal data must be limited to what is strictly necessary, stored securely, and anonymised or pseudonymised where feasible (covered in chapter 8 herein)

11.2.1 Data Protection Impact Assessments (DPIAs)

"A DPIA is a process designed to describe the processing, assess its necessity and proportionality and help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data[6] by assessing them and determining the measures to address them. DPIAs are important tools for accountability, as they help controllers not only to comply with requirements of the GDPR, but also to demonstrate that appropriate measures have been taken to ensure compliance with the Regulation (see also article 24)5. In other words, a DPIA is a process for building and demonstrating compliance."[7]

Under GDPR Article 35, a Data Protection Impact Assessment is required for any processing that is *"*likely to result in a high risk to the rights and freedoms of natural persons."[8] The regulation specifically enumerates high-risk cases that mandate a DPIA, including:

- Systematic, extensive automated profiling or decision-making that significantly affects individuals (Article 35(3)(a))
- Large-scale processing of special-category data (sensitive personal data as defined in Article 9, such as health, genetic, biometric data) or of personal data relating to criminal offenses (Article 35(3)(b))
- Systematic monitoring of publicly accessible areas on a large scale (e.g. extensive CCTV surveillance in public spaces) (Article 35(3)(c)) .

Beyond these explicit criteria, European guidelines (Article 29 Data Protection Working Party (WP29)/ European Data Protection Board (EDPB)) advise that a DPIA should be considered whenever multiple *high-risk factors* are present, for example, use of new technologies, tracking of individuals, processing data of vulnerable subjects, or combining datasets. Notably, the EDPB emphasises that introducing novel technology can itself trigger the need for a DPIA, since it may involve new forms of data use with potential unforeseen risks What this suggests in practice is that if a processing operation meets at least two high-risk criteria from the guidelines' list (e.g. it involves profiling and sensitive data, or monitoring and vulnerable subjects), a DPIA is strongly recommended even if not automatically mandatory. [9][10]

11.2.1.1 Recommendations on DPIAs and Ethical Procedures

The analysis of the DMP questionnaire revealed that:

- Most partners do not anticipate activities that clearly trigger the mandatory requirement for a DPIA.

- A few partners indicated uncertainty regarding the need for DPIAs.
- Two partners explicitly confirmed that they have already conducted DPIAs relevant to their activities within the Cynergy4MIE project

As previously outlined, the ethics compliance process involves reviewing partner responses from the DMP survey, with individual, private follow-up recommendations conducted by the EA. The EA will leverage information provided by partners, along with relevant EC procedures and GDPR regulations, to conduct structured evaluations and issue tailored recommendations. Although most partner responses currently do not definitively indicate mandatory DPIA requirements, the EA strongly advises partners involved in potentially high-risk activities to proactively perform DPIAs or detailed privacy risk assessments. This proactive approach ensures that data protection measures are integrated into all project stages, ensuring compliance by design and by default.

Proactively conducting DPIAs helps partners identify and mitigate potential privacy risks early, ensuring appropriate technical and organisational safeguards, such as encryption, pseudonymisation, informed consent procedures, and clearly defined data retention policies. DPIAs or detailed privacy risk assessments are particularly recommended for scenarios potentially involving:

- User profiling or processing of personal preferences data.
- Human-robot interactions and wearable sensor technologies.
- Emergency scenarios potentially involving health-related sensor data.
- Autonomous or smart-infrastructure sensor monitoring in public environments.

The EA, in collaboration with the PC, will actively support partners in identifying these scenarios and encourage proactive privacy assessments, ensuring compliance is built into project design and implementation.

Additionally, partners will also establish Data Processing Agreements (DPAs) when personal data is processed on behalf of another partner (as per GDPR Article 28) and to use Standard Contractual Clauses (SCCs) when transferring personal data internationally (GDPR Article 46). These are covered in the following sections.

11.2.2 International Data Transfers (Non-EU)

Cynergy4MIE involves collaboration with five partners located outside the EU, notably from the following non-EU countries:

- United States (1)
- Israel (1)
- Taiwan (2)
- Japan (1)

International transfers of personal data from EU-based consortium partners to these non-EU partners require specific safeguards to ensure full compliance with GDPR's Chapter V (Articles 44-50), explicitly governing international data transfers. Additionally, some EU-based partners explicitly confirmed transfers involving non-EU countries.

The European Commission has issued **adequacy decisions** recognising certain non-EU countries as providing sufficient data protection standards equivalent to GDPR. Among Cynergy4MIE non-EU partners, the following adequacy statuses apply:

- **Israel:** Recognised as having adequate protection by an EU Adequacy Decision. Personal data may be transferred freely without additional safeguards beyond compliance with internal consortium ethics and GDPR principles.

- **Japan:** Recognised under the EU-Japan mutual Adequacy Decision. Transfers of personal data can also occur freely under this framework, provided, as mentioned above respective partners remain compliant with applicable Japanese data protection legislation aligned with internal consortium ethics and GDPR principles.

For the other non-EU countries involved:

- **United States:** Currently, the United States (US) does not have a general adequacy decision. To transfer personal data lawfully from the EU to the US, Cynergy4MIE consortium partners must implement GDPR-approved transfer mechanisms, such as the SCCs, to ensure compliance and safeguard data subjects' rights.
- **Taiwan:** Similarly, Taiwan does not hold an EU adequacy decision. Transfers to Taiwanese partners must similarly be based on SCCs or another appropriate safeguard as provided under GDPR Chapter V, to maintain legal compliance.

Some important relevant clarifications are provided below.

Do non-EU partners need to comply with GDPR?

- GDPR's territorial scope (Article 3 GDPR) applies explicitly to entities established in the EU or entities outside the EU that process personal data of EU individuals by:
    - Offering goods or services to EU residents (Article 3(2)(a)), or
    - Monitoring the behaviour of individuals within the EU (Article 3(2)(b)).
- What this suggests in practice:
    - Non-EU partners (from the USA, Israel, Taiwan) **do become subject to GDPR if they handle personal data related to EU individuals**, especially if the data collection involves research participants or data from EU-based activities.
    - However, **if a non-EU partner handles personal data exclusively from non-EU sources, collected entirely outside EU territory and unrelated to EU persons**, they generally **are not directly obliged under GDPR**. (In practice, this scenario is rare in Horizon projects involving EU beneficiaries, since data typically flows across consortium partners)
        - Nevertheless, as soon as **EU partners** receive and process that data in the EU, **those EU partners become controllers** under GDPR, and therefore GDPR rules **do apply** to them, including DPIA requirements if relevant.

EU to non-EU data transfers:

Under GDPR Chapter V (Article 46), whenever personal data originates in the EU and is transferred to a country without an EU adequacy decision (USA, Taiwan), SCCs or other suitable GDPR transfer safeguards must be applied.

- Therefore, any EU partner sending personal data to USA and/or Taiwan must ensure that appropriate safeguards, such as SCCs, are formally in place and documented.

Non-EU to EU data transfers:

When data originates from a non-EU partner and is transferred into the EU, GDPR doesn't explicitly mandate SCCs or similar safeguards for incoming data, provided:

- Data collection and initial processing occurred entirely outside the EU.
- The EU receiving entity becomes the controller upon receipt, and thus compliance obligations are governed by their internal GDPR compliance processes once the data arrives in the EU.
- For partners in countries with adequacy decisions (Israel, Japan):

- Transfers between EU and these countries are simpler. The adequacy decision ensures a simplified and compliant transfer without needing additional safeguards like SCCs.

Thus, to clearly summarise the above points:

- Transfers **from the EU to the US and Taiwan** require SCCs explicitly.
- Transfers **from the EU to Israel and Japan** do not require SCCs, thanks to adequacy decisions.
- Transfers from **non-EU (US/Taiwan) into the EU** don't strictly require SCCs (or similar) under GDPR but still require careful internal data handling procedures to ensure GDPR compliance once data enters the EU.

In practical terms, Cynergy4MIE partners who transfer personal data to USA and Taiwan will proactively formalise and maintain SCCs or another appropriate safeguard, clearly detailing their responsibilities and obligations regarding data transfers and protection standards. In addition to the guidelines provided here and in D9.1, and any relevant follow-up recommendations following the DMP survey responses from the EA and PC, partners will consult their internal legal and/or data protection advisors to finalise these SCCs, ensuring appropriate protection measures and clearly defined responsibilities.

11.2.3 Data Processing Agreements (DPAs)

As analysed in chapter 8 of this deliverable, whenever one partner processes personal data on behalf of another within the consortium (regardless of geographical location), DPAs in compliance with GDPR Article 28 are mandatory. These DPAs must define clearly and contractually:

- The scope, purpose, and duration of processing activities.
- Specific data security measures.
- Obligations related to data subject rights.
- Conditions for data deletion or return after processing concludes.

Consortium partners involved in such processing will formalise DPAs to clearly delineate data protection responsibilities.

11.3 Data Protection Coordination Process in Cynergy4MIE

As mentioned in the previous section, after evaluating the partners' responses to the DMP questionnaire and discussions between the EA and PC, it was concluded that a dedicated consortium-level DPO for Cynergy4MIE is not required at this stage, as GDPR obligations related to data protection are comprehensively covered at the partner level. Partners either already have their own internal DPOs (mandatory for public institutions and certain large organisations) or designated data management experts explicitly responsible for GDPR compliance. Those partners who have not explicitly appointed a DPO have generally identified a data management lead or expert responsible for GDPR compliance and DPIA determinations.

The PC and EA, based on the DMP questionnaire responses, maintain a confidential list of contacts from all beneficiaries with their respective DPOs or designated data management experts. This list will be used solely for internal communication and coordination purposes regarding data protection issues.

It is important to clarify that this coordination process is intended as a two-way support mechanism. The PC, along with the EA when relevant, will provide general guidance and practical support to partners whenever necessary. D9.1 clearly outlines the procedures for communicating and reporting ethics-related and data protection issues, specifically sections “6.6.3.1 Ethics Issue Reporting Protocol” and “Annex C: Ethics Issue Reporting and Assessment Template for Cynergy4MIE”.

However, it is emphasised that each partner retains full individual responsibility for ensuring GDPR compliance. While internal consortium resources, including guidance from the EA and PC, are available for support and clarification, such support does not constitute legally binding advice. For formal legal or specialised data protection guidance, partners should consult their internal DPOs, legal teams, or external data protection experts as needed.

Lastly, the EA of Cynergy4MIE provides general ethical oversight and guidance on ethical standards relating to data protection within the project. However, the EA explicitly does not serve as a DPO, nor provides legally binding data protection advice. Each consortium partner retains sole responsibility for ensuring compliance with GDPR, including the appointment of DPOs, conducting DPIAs when necessary, and obtaining formal legal counsel or expert data protection advice as appropriate.

11.4 Ethics Compliance Monitoring

As aforementioned, Cynergy4MIE implements structured internal checklists and reporting templates detailed explicitly in D9.1 to proactively monitor and address ethics-related issues. These mechanisms include:

- **Ethics Issue Reporting Protocol (D9.1, Section 6.6.3.1)**: clearly describing how partners should report ethics-related issues or concerns.
- **Ethics Issue Reporting and Assessment Template (D9.1, Annex C)**: a structured template for partners to systematically document and submit ethics concerns to the EA and PC for internal assessment and response.

The ethics framework outlined in D9.1 will guide the development and implementation of subsequent deliverables and processes, ensuring the dynamic refinement of the project's ethical governance. Specifically:

- **Data Management Plan (D8.2 and D8.7)**: These deliverables will play a pivotal role in refining ethical practices accordingly. Insights from the DMP will inform updates to the ethics framework in D9.2, D9.3, and D9.4.
- **Periodic ethics reviews**: WP9 deliverables, including D9.2 (M12), D9.3 (M24), and D9.4 (M36), will reflect updates based on ongoing project activities, emerging challenges, and feedback from consortium partners. These reviews will ensure the ethics framework remains responsive to new ethical considerations.
- **Ethics workshop**: An internal ethics workshop will be held during the upcoming General Assembly meeting (25–26 June 2025) to enhance partners' understanding of the ethics framework and support its consistent application across all work packages. The content of the workshop will directly relate to D9.1 and the insights gained from DMP survey to offer useful practical knowledge and application directly relevant to Cynergy4MIE's scope.

11.5 Gender and Inclusivity Monitoring

Cynergy4MIE is committed to promoting gender equality and ensuring inclusive participation across all phases of the project. In alignment with Horizon Europe's priorities and the European Commission's Guidance on Gender Equality Plans, the project supports equal opportunities and diverse representation in research, development, leadership, and technical decision-making.

Where relevant, Cynergy4MIE will monitor and promote gender balance in participant recruitment, stakeholder engagement, simulation studies, and demonstrator-based field trials. While recognising

that technical constraints or small sample sizes may limit representation in specific cases, the consortium will actively strive for inclusivity in all research contexts and knowledge-sharing activities.

By integrating these considerations into both planning and data practices, Cynergy4MIE contributes to a responsible and inclusive innovation ecosystem.

The Cynergy4MIE consortium recognises that ethical governance is a continuous process. Through regular reviews, partner engagement, and proactive measures, the consortium will ensure full compliance with EU ethical standards while supporting innovation and societal impact.

[1] Deliverable 9.1 "EPQ - POPD - NEC - H - AI – Requirement No. 1", HORIZON JU Research and Innovation Actions Project "Cynergy4MIE", Grant Agreement 101140226, submitted: M3.

[2]https://commission.europa.eu/law/law-topic/data-protection/rules-business-and-organisations/obligations/data-protection-officers/does-my-companyorganisation-need-have-data-protection-officer-dpo_en

[3] https://gdpr.eu/data-protection-impact-assessment-template/

[4] https://gdpr.eu/what-is-data-processing-agreement/

[5] https://gdpr.eu/article-46-appropriate-safeguards-personal-data-transfers/

[6] The GDPR does not formally define the concept of a DPIA as such, but

- its minimal content is specified by Article 35(7) as follows:

- "*(a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;*
- *(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;*
- *(c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and*
- *(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned";*

- its meaning and role is clarified by recital 84 as follows: "*In order to enhance compliance with this Regulation where processing operations are likely to result in a high risk to the rights and freedoms of natural persons, the controller should be responsible for the carrying-out of a data protection impact assessment to evaluate, in particular, the origin, nature, particularity and severity of that risk".*

[7] https://ec.europa.eu/newsroom/article29/items/611236

[8] https://gdpr-text.com/read/article-35/#related_gdpr-a-35_3b

[9] https://www.edpb.europa.eu/our-work-tools/general-guidance/endorsed-wp29-guidelines_en

[10] https://ec.europa.eu/newsroom/article29/items/611236

12 Conclusion

The Consortium Agreement (CA) includes provision for data management as agreed between the project partners, and the Grant Agreement (GA) include provisions for data management obligations as agreed with the European Commission. However, good data management also requires best practice guidance and project level processes.

This DMP provides this guidance and best practice.

Execution of the DMP (Data Management Plan) is the responsibility of all project members relative to their roles and responsibilities. The Project Coordinator (PC), Work Package (WP) leaders, Supply Chain (SC) and Task leaders, will provide wide reaching project support to implement the DMP and provide additional support where required.

It should be noted that the DMP is in no way a substitute for the project's legal documents and do not replace their enforcement in any way – if in doubt the legally binding documentation takes precedence.

The DMP identifies the FAIR principals as a key guiding point to ensuring data is findable, accessible, interoperable and repeatable. The principals are summarised in the DMP along with an explanation of Cynergy4MIE's commitment to align with these principals. The Cynergy4MIE project will follow the FAIR principals where possible, relative to commercial and practical restrictions.

The way in which data is handled and disseminated, is of the upmost importance. The project brings together a wide range of partners with different internal processes and objectives, from commercial, to technology and research. It is essential that a common understanding of how data is handled, the conditions under which data is made public and the processes of agreeing such conditions is established and maintained. In doing so, a culture of trust can be established which in turn will enhance the collaboration of the partners, and ultimately the project outcomes. Whilst the day-to-day interactions between partners and the appropriate employment of due diligence is what builds such trust, the DMP provides guidance and recommendations on best practice.

This includes guidance on:

Identifying Data Originators: The data originator is the organisation that originally created the data. Unless otherwise and explicitly stated it should be assumed the Data Originator owns the data and has the authority and responsibility to define who that data can be shared with, for what purpose and its classification.

Best practice processes for managing data including:

- **Classifying data**
- **Labelling data**
- **Processes for public dissemination**
- **Key contact points**

In the preparation of the DMP, all project partners were consulted via a questionnaire. The structure of this questionnaire together with its outcomes, in the form of a definition of data themes and data types are provided.

It should be noted that a substantial component of the overall project is the creation of a data framework. This forms the deliverables in WP5 and WP6, with other work packages contributing. The specific data management policies developed within these WP's and for the framework itself fall outside of this DMP, as they will require substantial and specific consideration. Nevertheless, the principles and guidelines set out within this DMP, will act as an initial framework to inform the development of the data framework.

If you are, or think you maybe, dealing with personally identifiable data you will be classed as a 'data controller' under GDPR. Whenever any project member intends on collecting, processing, or using personally identifiable data of any kind, GDPR and other legal compliance requirements must first be considered.

This DMP provides:

- **The key definitions** (Personal data, Data processing, Data subject, Data controller, Data processor)
- **The key principals** that should be followed (Lawfulness, fairness and transparency, Purpose limitation, Data minimization, Accuracy, Storage limitation, Integrity and confidentiality, Accountability)
- **Accessing further guidance**

As soon as partners are aware data and findings are of public value, they will begin, in accordance with the guidance in this plan and the terms of the CA and GA, exploring the possibility of making that data public. The DMP provides best practice guidance and processes for making data available within the project and in order that that data be maintained and available beyond the time frame of the project.

Finally, the Cynergy4MIE project is forecast to use several data depositories. In all instances, project partners will follow best practices in selecting, implementing and maintaining data storage facilities.

Ethical compliance is an integral aspect of data management in Cynergy4MIE. The DMP works in alignment with the ethics framework established in D9.1 and includes proactive measures such as risk assessment templates, consent protocols, and ethics issue reporting processes. The integration of ethics-related questions into the DMP survey further supports ongoing monitoring, with findings informing both WP8 and WP9. This reinforces the consortium's commitment to responsible research, ensuring that all data-related activities respect privacy, integrity, transparency, and legal compliance in accordance with GDPR and Horizon Europe principles.

13 References

1. Cynergy4MIE Consortium (2024). Cynergy4MIE Consortium Agreement.
2. Cynergy4MIE Consortium (2024). Cynergy4MIE Grant Agreement.
3. Cynergy4MIE Consortium (2025). Cynergy4MIE Amendment.
4. Cynergy4MIE Consortium (2024). Cynergy4MIE Handbook.
5. FAIR Principles - GO FAIR (go-fair.org)
6. https://osf.io/dp6je/
7. https://zenodo.org/
8. H2020 Programme: Guidelines to the Rules on Open Access to Scientific Publications and Open Access to Research Data in Horizon 2020.
9. https://open-research-europe.ec.europa.eu/
10. https://ec.europa.eu/research/participants/docs/h2020-funding-guide/cross-cutting-issues/open-access-data-management/data-management_en.htm
11. https://schema.datacite.org/meta/kernel-4.4/doc/DataCite-MetadataKernel_v4.4.pdf
12. https://schema.datacite.org/meta/kernel-4.4/doc/DataCite-MetadataKernel_v4.4.pdf
13. https://schema.datacite.org/meta/kernel-4.4/
14. https://datacite.org/
15. https://gdpr.eu/what-is-gdpr/

14 Appendix: Cynergy4MIE Consortium Data Management Plan

The purpose of the Cynergy4MIE questionnaire is for project partners to provide their data management strategy for allocated resources, data generation, data storage, accessibility, security, data re-use and ethics.

The Cynergy4MIE questionnaire can be found here.

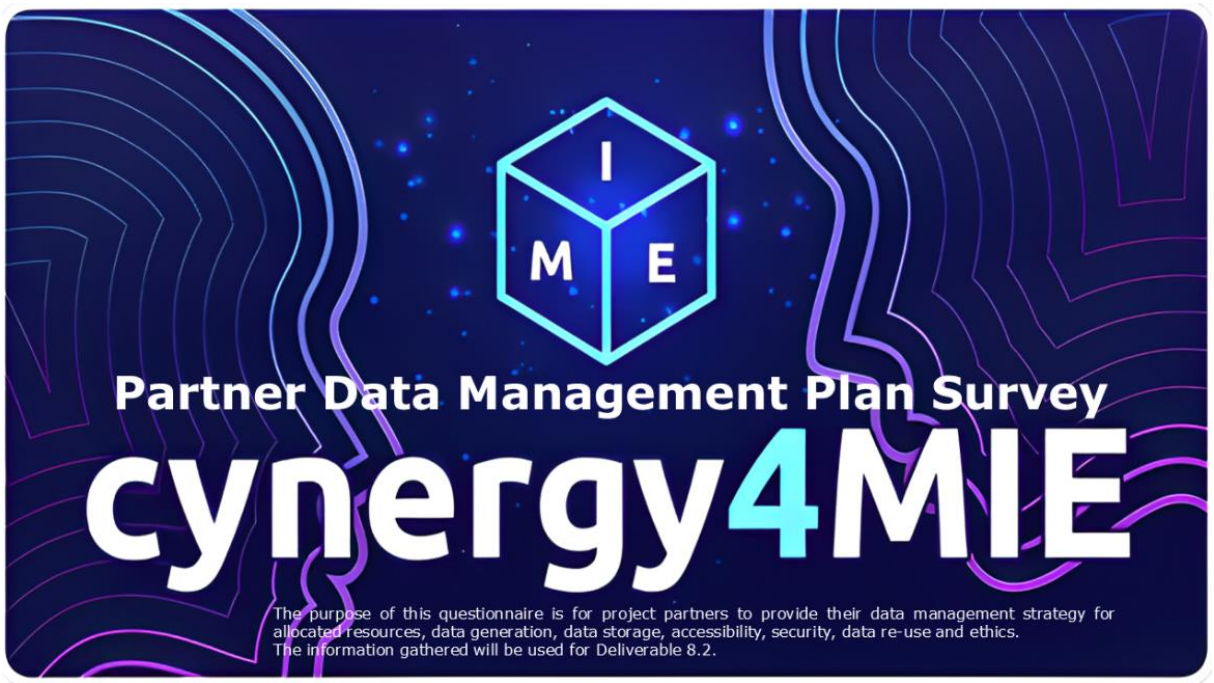

FIGURE 12: CYNERGY4MIE PARTNER DATA MANAGEMENT PLAN - HOME-PAGE

14.1 General information

The Data Management Questionnaire stores the following information for each participant of the survey:

ID	Progressive identification number
Startzeit	Time survey startet
Fertigstellungszeit	Time survey ended
E-Mail	E-Mail address of participant (can be anonymous)
Name	Name of participant (can be anonymous)
Language	Language selected
Zeitpunkt der letzten Änderung	Time of last changes

14.2 Participant's input

The full Questionnaire of the ARCHIMEDES Data Management Plan is given in Table 7.

TABLE 7: CYNERGY4MIE DATA MANAGEMENT PLAN QUESTIONNAIRE

Participant Information
1. What ist the name of your organization?
2. What is your role in the project?
3. Please provide your name and email so we can contact you if any clarifications are needed regarding your responses. (If multiple people contributed to this response, please list the main contact person.)
Resources & Costs
4. Who decides how and which data will be kept and for how long? (Please add name, last name, position and E-Mail)
5. What will be the costs for making data or other research outputs findable, accessible, interoperable and reusable – FAIR – in Cynergy4MIE? (e.g. direct and indirect costs related to storage, archiving, re-use, security, etc.)
6. In regards to the previous question, please explain how the necessary resources have been costed in.
7. How will these costs be covered? Note: costs related to research data/output management are eligible as part of the Horizon Europe grant (if compliant with the Grant Agreement conditions).
Data – General Information
8. Which type and format will generated data in the scope of your tasks and demonstrators have? (on partner level)
9. What is the purpose of data generation or re-use and its relation to the objectives of the project?
10. What is the expected size of the data that you intend to generate or re-use? (If not a precise figure at least an order of magnitude)
11. To whom might your data be useful outside of the Cynergy4MIE project?
Metadata
12. Which metadata will be created in the scope of your tasks and demonstrators?
13. Will metadata be collected and indexed?
14. Will a documentation or reference about any software that is required to access or read the data be included?
15. Will it be possible for your organization to include the relevant software (e.g. in open source code)?
16. Will metadata contain information to enable the user to access the data?
17. Will metadata vocabularies, standards, formats or methodologies be followed?
18. In case metadata standards do not exist in your discipline, please outline what type of metadata will be created and how.
Data Storage, Access & Security
19. Will the data be safely stored in trusted repositories for long term preservation and curation?
20. With reference to the previous question, where will the data be stored?
21. What methods or software tools are needed to access and use data?
22. Which provisions are or will be in place for data security (including data recovery as well as secure storage/archiving and transfer of sensitive data)?

23. Does the repository ensure that the data is assigned with an identifier?
24. Have you discussed and considered the terms and conditions that will apply for archiving and storage of data? For example: Security, Privacy, Availability, Rights and Accessibility
25. If you have answered yes to the previous question, please specify what are the terms and conditions established for archiving and storing of your data?
26. Please select accordingly what applies to your data availability:
27. How long will your data remain available and findable?
28. Is any data known that will be made open access (e.g. publication, deliverables, other data for tests and experiments)?
29. If you have answered yes to the previous question, please specify which data will be made open access.
30. Will the data be accessible through a standardized access protocol?
31. If you have answered yes to the previous question, please specify the standardized access protocol to be used.
32. If there are restrictions on use, how will access be provided to the data, both during and after the end of the project?
33. In case it is unavoidable that you use uncommon or generate project specific ontologies or vocabularies, will you provide mappings to more commonly used ontologies?
34. Will you openly publish the generated project specific ontologies or vocabularies to allow reusing, refining, or extending them?
Third Parties & Data re-use
35. Will the data produced in the project be usable by third parties, in particular after the end of the project?
36. Will some data be re-used in different demonstrators/use cases and by different Cynergy4MIE project partners?
37. Will data from other sources (Other projects, other Demos in the Cynergy4MIE,…) be re-used?
38. If you have answered yes to the previous question, please specify in which format the data will be re-used?
39. How will you provide documentation required to validate data analysis and facilitate data re-use? (e.g. readme files with information on methodology, codebooks, data cleaning, analyses, variable definitions units of measures, …)
40. Is your usage of data from other sources affecting any IP?
41. How will other legal issues, such as intellectual property rights and ownership, be managed?
Legal & Ethics GDPR & Personal Data Protection
42. What types of data does your organisation collect and process for Cynergy4MIE? Please explain why each type of data is necessary for the project and how you ensure that excessive or unnecessary data is not collected (in line with the data minimisation principle)
43. Will you handle "special categories of personal data" (racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data, sex life or sexual orientation)?
44. If you answered yes in question 43., briefly justify why.

45. Will you obtain consent from the related data subjects/research participants for processing their personal data? If not, specify the legal basis (e.g., legitimate interest, contractual necessity, public interest).
46. Will you process previously collected personal data (secondary use)? If so, please describe the data and justify your right to use data for this project (e.g., consent).
47. What specific GDPR-compliant technical and organisational measures are in place to safeguard the rights and freedoms of data subjects/research participants? (Check all that apply) ○ Access control (restricted access to authorised personnel, role-based permissions) ○ Secure storage (e.g., encrypted databases, controlled cloud access with GDPR-compliant providers) ○ Data retention policies (automatic deletion after retention period, minimisation of stored data) ○ Regular security audits and GDPR compliance checks ○ other
48. If you answered "other" in Question 47., please specify here.
49. How can participants request deletion of their personal data in accordance with GDPR? (e.g., formal written request, online form submission).
50. Which privacy-preserving techniques have been or will be applied to ensure data security and limit unnecessary exposure of personal data? (Check all that apply.) ○ Anonymisation (removal of personally identifiable information to prevent re-identification) ○ Pseudonymisation (substituting identifiable data with pseudonyms while maintaining traceability under controlled access) ○ Encryption (secure encryption for both data at rest and in transit) ○ Synthetic data generation (creating artificial datasets that retain statistical properties of real data) ○ Access control and role-based permissions (minimising who can access sensitive data) ○ Federated Learning / Secure Multi-Party Computation (MPC) (privacy-preserving machine learning across distributed data sources) ○ other
51. If you selected "other" in Question 50., please specify here.
Legal & Ethics Data Sharing
52. Will data be transferred outside the EU or from a non-EU country to an EU country/partner (e.g., Israel, Taiwan, USA)? ○ Yes ○ No
53. If you answered yes in Question 52., please specify which legal framework ensures GDPR compliance: Standard Contractual Clauses, adequacy decisions, etc.
Legal & Ethics GDPR Risk Assessment & Compliance
54. Does your data processing require a Data Protection Impact Assessment (DPIA) under GDPR? ○ Yes – A DPIA has been conducted. ○ Yes – A DPIA is required but not yet conducted. ○ No – A DPIA is not required. ○ Not sure – Need further assessment.
55. If you answered "No – A DPIA is not required" in Question 54., please provide a justification for why a DPIA is not needed.
56. Who is responsible for determining whether a DPIA is required for your organisation's data processing activities within the Cynergy4MIE project? Response options:

• Same as answered in Question 4. • Different contact, then please provide name, position, and email
57. Does your organisation have policies or external requirements that govern how you manage research data (e.g., national laws, funder requirements, sectoral standards)?
58. Are there any ethical or legal issues that can have an impact on data sharing (e.g., confidentiality agreements, IP restrictions, data sensitivity)?
Legal & Ethics Environmental & Safety Considerations
59. Are there any potential environmental or safety risks associated with your research activities? If there are, specify risk mitigation measures, e.g., sustainable materials, safety protocols.
Legal & Ethics Ethical AI
60. Does your dataset contribute to AI-based decision-making? If it does, describe how fairness, bias mitigation, and transparency are ensured

15 List of figures

16 List of tables

17 Internal review

	Reviewer 1: Claudio Caramaschi	Reviewer 2: Haris Isakovic

1. Is the deliverable in accordance with:

		Answer	*Comments*	*Type**	*Answer*	*Comments*	*Type**
(i)	the description of work?	yes		M/m/a	yes		M/m/a
(ii)	the international state of the Art?	yes		M/m/a	yes		M/m/a

2. Is the quality of the deliverable in a status that:

		Answer	*Comments*	*Type**	*Answer*	*Comments*	*Type**
	allows to send it to Chips JU?	yes		M/m/a	yes		M/m/a
(ii)	needs improvement of the writing by the originator of the deliverable?	no		M/m/a	no		M/m/a
(iii)	needs further work by the partners responsible for the deliverable?	no		M/m/a	no		M/m/a

* Type of comments: M = major comment; m = minor comment; a = advise

- Last page of the document is intended to be blank! -