DiCiM

Digitalised Value
Management for Unlocking
the potential of the Circular
Manufacturing Systems with
integrated digital solutions

D9.2 INITIAL DATA MANAGEMENT PLAN

Project 101091536

Funded by
the European Union

D9.2 Initial data management plan

Project acronym:	**DiCiM**
Project full title:	**Digitalised Value Management for Unlocking the potential of the Circular Manufacturing Systems with integrated digital solutions**
Grant agreement no.:	**101091536**
Author/s:	**Alena Klapalová (MUNI)**
Reviewed:	**Michael Bolech (C-ECO), Ruud de Bruijckere (SIG), Mario Lorenz (TUC), Sayeed Shoaib Ul Hasan (KTH)**
Approved:	
Document type:	**DMP (data management plan)**
Dissemination Level:	**PU**
Version:	**3**
Date:	**29th June 2023**

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

Funded by the European Union

History of Changes

Version	*Date*	*Modification reason*	*Modified by*
V1.0	01 06 2023	Initial Draft	Alena Klapalová
V1.0	05 06 2023	Full report review	Michael Bolech (C-ECO)
V1.0	09 06 2023	Full report review	Sayeed Shoaib Ul Hasan (KTH)
V1.0	20 06 2023	Full report review	Mario Lorenz (TUC)
V1.0	26 06 2023	Full report review	Ruud de Bruijckere (SIG)
V2.0	27 06 2023	Semifinal reviewed deliverable	Alena Klapalová (MU)
V2.0	28 06 2023	Semifinal full report review	Mario Lorenz (TUC)
V2.0	28 06 2023	Semifinal full report review	Ruud de Bruijckere (SIG)
V3.0	29 06 2023	Final report	Alena Klapalová (MU)

Funded by
the European Union

Table of Contents

Funded by the European Union

Managed document

Version number	1	**Prepared by:** **When:**	Alena Klapalová (MUNI) 1st June 2023
Number of pages	45	**Verified by:** **When:**	
Number of annexes	3	**Approved by:** **When:**	
Date	1st June 2023	**Valid from:**	
Description of change(s) (chapter, page, No of Fig., Table, Graph if relevant)	none		

Funded by the European Union

List of Figures

Funded by
the European Union

List of Tables

Funded by the European Union

List of Abbreviations

Abbreviation	*Explanation*
CA	Consortium Agreement
CMS	Circular Manufacturing Systems
CVM	Circular Value Model
DiCiM	Digitalised Value Management for Unlocking the potential of the Circular Manufacturing Systems with integrated digital solutions
DMP	Data Management Plan
DoA	Description of Action
DOI	Digital Object Identifier
EDI	European Data Infrastructure
EOSC	European Open Science Cloud
FAIR	Findable, Accessible, Interoperable, Usable
GA	Grant Agreement
GDPR	General Data Protection Regulation
ICT	Information and Communication Technology
IDMP	Initial Data Management Plan
IPR	Intellectual Property Rights
ORCID	Open Researcher and Contributor IDentifier
PI	Principal Investigator
PID	Persistent Identifier
PU	Public Deliverable
R&D	Research and Development
SEN	Sensitive deliverable
WP	Work Package

1. Executive Summary

Deliverable D9.2 “Initial Data Management Plan” (also IDMP or DMP) describes the objectives and requirements of managing the data that will be generated, formatted, collected, analysed, stored, preserved, protected, shared and licensed (and other associated processes) during the course of the project and for a specified period after its completion. This document provides guidance for consortium members and relevant parties on **what** data will the project work with and **why** as well as **who**, **what** and **how, where and when** will realize the above introduced processes related to data.

This deliverable was prepared using structure and a check-list containing guiding questions of the Horizon Europe Data Management Plan Template, Version 1.0, released on 5 May 2021 (available here: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/how-to-participate/reference-documents;programCode=HORIZON). For the design of the IDMP FAIR (findability, accessibility, interoperability and re-usability of data) principles have been followed. These principles will be followed for any updated version of DMP.

The content of the Deliverable adheres to the requirements and recommendations provided within the guidelines in the Article 17 of the AGA — Annotated Grant Agreement. It also follows the rules stated in chapter 4 *Grant Implementation*, *Decription of Action (Part A), Part* B (chapters 1.2.6, 1.2.7, 2.1.5 and 2.2.3 as well as chapter 4 related to ethics) and *Annex 5* of consortium Grant Agreement (also GA) and chapters 4.4, 8 and 9 of Consortium Agreement (also CA).

DMP as a living document will be updated during the project implementation taking into account changes in methodology, type of data, formats, costs or management (or other changes not specified in the proposal and agreements) and new data and information. The final version will be delivered in M48. DMP is a managed document and as such every change should be recorded in a new version with a new version number, clear description of changes and with verification and approval of the responsible persons. A table for managed document is included also in this IDMP (p. 4 “Managed document”).

Objectives of data management are presented in chapter 2. What data is involved in this project and background information on data management is covered in chapter 3. FAIR principles application to data and data management is described in chapter 4. What and how other research outputs will be treated is outlined in chapter 5. Allocation of resources in terms of costs and responsibilities is introduced in chapter 6. Chapters 7 and 8 cover the concerns of data security and ethics. The chapter related to the ethics follows basic elements of this plan what means to answer to the basic questions (what, why, who, when, where and how). The reason for this approach is that ethics concerns all points and information introduced in the previous chapters. Final chapter is dedicated to the conclusions and an outline of the next steps.

Funded by
the European Union

2. Introduction and Objectives of the Data Management and Initial Data Management Plan

This deliverable is the result of the Task 9.3, which is the part of WP9 "Project management". Objectives of the task translated into the content of the deliverable are as follows:

- ✓ Outline a data management plan that includes:
  - Information on the handling of research data during & after the end of the project (what data will be collected, processed, and generated, which methodology & standards will be applied, whether data will be shared/made open access and how data will be curated & preserved);
  - Setting up open access repository for data and publications in the project. For the open access to the research data, the open access commitment described in section 1.2.6 of the GA, according to Plan S (initiative concerning scientific publications launched by Science Europe) and the FAIR principles (findable, accessible, interoperable, and reusable) of open access publishing must be followed.

Except for the objectives defined in the Task 9.3, one of the objectives of the WP9 itself needs to be added, which is to monitor and evaluate the social impact of the project – in the case of data management this means particularly data privacy and ethics.

Data management methodology and tools have been agreed by consortium partners and are summarised in Table 11, p. 20, part B of the Grant Agreement.

2.1. Background and objectives of the project

The DiCiM project is focused on working with data and information, especially data in the context of the digital and circular economy. Its key objectives are based on data generation, data flow, data analysis as well as data integration and finally on data application and use in industrial practice. The ultimate objectives are to digitise existing demonstrators´ data (if existing and usable for the project), to digitise the processes that generate, format, analyse, integrate, share, store, preserve and secure data, and to create integrated digital solutions that combine open access digital platform for lifecycle information management and support solutions for value recovery activities for demonstrators and relevant stakeholders along the circular value chain (Key area I), prepare training materials for the employees and to demonstrate with the help of trained personnel viability of both new technologies and platform. Licensing of the project results is also one of the objectives which requires data management. The open access digital platform will be developed with the objective to enhance data sovereignty, decentral data management, data economy and data governance together with data security, privacy and compliance. Digitalized processes help to achieve efficiency and responsiveness in the value recovery activities and to enable reuse of products, parts and materials.

These data processes will be realized not only by demonstrators and ICT developers (2 groups of consortium partners). Within demonstrators, different functions are involved in the form of cross-functional integration (e.g. product designers, logistics and supply chain management, sales, services, returns management) related to the circular manufacturing systems (CMS) and

Funded by the European Union

circular value model (CVM) so there will be business cases with a business model around and through data processes. Digitalization of data and data flow will be provided through the work of demonstrators and ICT firms and ICT developers from universities who are consortium partners. Also, external stakeholders beyond the consortium along the supply chains (e.g. suppliers, logistics and repair service providers, core brokers) will be engaged into some data processes concerning the core of the project. Research data will be produced, processed and shared also by two other partners from universities (KTH and MUNI) and by the communication and dissemination partner (CHX).

Additional data and information will be generated from and around these data and data streams that will not be applied directly to the demonstration of the project objectives by the demonstrators. If relevant, all the requirements for data security will be applied.

2.2. Objectives of data management and brief description of actions

The objectives of any data management typically include issues of:

Data governance and lifecycle management - establishing policies, procedures, and guidelines for the proper management, access, and use of data throughout the project life and beyond. This includes defining roles, responsibilities, and accountability for data-related activities, establishing data retention policies, specifying the criteria for data retention or disposal, and ensuring compliance with legal and regulatory requirements. (Alhassan et al, 2016; Sinaeepourfard et al, 2016; Al-Badi et al, 2018; Rahul and Banyal, 2020).

All points below are data governance and data lifecycle management content. In the **DiCiM project** data reused, produced and further processed belong to the partners of the consortium, more specifically to those who generate the data. Conditions of the ownership of the data (and research results), protection, transfer and licensing are specified in Annex 5 of the GA, Article 16. Dissemination and exploitation of the results in the Article 16 and 17 of the Annex 5 of the GA are also part of the Communication and Dissemination plan and its updates (D8.2). Data governance will be described in more details in chapter 6.2 and chapter 8.

- *Data quality and quality assurance* – ensuring the accuracy, completeness, consistency, and validity of data throughout its lifecycle. This involves outlining strategies and procedures to prevent data errors, duplicates, and inconsistencies and may include measures such as data validation, cleaning, and error checking processes, as well as documenting any data quality assessments or limitations. (Eppler and Helfert, 2004; Haug et al, 2011; Gao et al, 2016; Wang et al, 2016).

In the DiCiM project these requirements are and will be met through the GA and CA, development and updating of DMP, through conscious planning of the type of data collection and further processes as for instance validation of collected and analysed data from co-creation workshops (WP1), from the technologies development and implementation phases, by review processes of deliverables and other text aiming to be published for both internal and external audience (see also D9.1 Project Quality Handbook – PU and D8.2 Dissemination and communication plan - SEN).

- *Data organization, structure and documentation* - defining a clear and consistent structure for organizing and formatting data. This includes establishing naming

Funded by
the European Union

conventions, file organization schemes, and data models that ensure data consistency and ease of use. This issue also means documenting essential information about the data, such as its origin, collection methods, variables, units of measurement, and any transformations or processing applied. This documentation helps ensure data understanding, reproducibility, and proper interpretation (Strasser et al, 2012).

In the DiCiM project first work on data organization, structure and documentation started before the project (content of deliverables and consistency and coherence between research outputs and packages). The project coordinator created a structured space for organizing the research and management outputs in the consortium internal repository (Microsoft Teams, further also MS Teams). Too organize, structure and document data generated within the individual tasks is also the role for all WP leaders and Tasks leaders throughout the duration of the whole project. PID will be allocated to the relevant objects and persons in every respective case by the individual beneficiary or designated person or authority.

- *Data analytics, integration and insights* - integrating data from various sources and systems to create a unified and consistent view of information. This may involve data cleansing, transformation, and consolidation to ensure compatibility and interoperability. These issues enable data-driven decision-making and deriving meaningful insights from data. The already mentioned data organizing and structuring should be done in a way that supports analytics, implementing data analytics tools and techniques, and facilitating data exploration and visualization. (Phillips-Wren et al, 2015; Grover et al, 2018; Walls and Barnard, 2020).

In the DiCiM project all these issues are part of the research work on the project objectives or even the essence of the whole project. This means that the knowledge of what data and how to analyse and integrate them and how to make the needed insights for those who have or may have interest has been discussed, thought out and planned already in the design phase of the project proposal. If any changes in the methods occur, the discussion will be organized by the relevant and competent WP and/or Task leader about the suitability, opportunities, benefits and barriers of the possible methods and techniques or tools for data analysis, integration and insights. Results will be documented in Minutes of Meetings and if important and needed also in the respective deliverable or any other type of outputs.

- *Data security, privacy and compliance* - protecting data from unauthorized access, use, disclosure, alteration, or destruction. This involves implementing security measures such as access controls, encryption methods, data anonymization techniques, as well as addressing legal and ethical requirements related to data privacy, backup and recovery processes, and regular security audits. Ensuring compliance with relevant data management policies, regulations, and funder requirements concerning the data protection regulations and privacy laws means to identify any specific requirements or guidelines imposed by funding agencies, institutions, or regulatory bodies (for instance in the EU the General Data Protection Regulation (GDPR)), and to incorporate them into the data management plan. This includes obtaining appropriate consent, managing data retention periods, and providing individuals with the right to access, modify, or delete their personal data. (Georgiadis and Poels, 2021; Mahanti and Mahanti, 2021; Schäfer et al, 2022).

Most of these issues have been considered already in the phase of preparing the proposal of the **DiCiM project** and how to tackle them is part of the CA (access rights to the background information in the Attachment 1), GA (Article 13, 15 and 16) and this deliverable. To monitor the development of legislative and other types of requirements and rules concerning data security and privacy and threats of a non-compliance and to take into account new situations is the job of WP and/or Task leaders. All the new facts will be discussed during regular and irregular WP meetings, General assemblies and meetings of the Executive Board and Advisory Board.

Potential challenges and risks of new legislations and other type of similar requirements and rules are already covered and will be followed and documented in the lists of risks which is part of the formal document *Minutes of Meeting* and according to the CA this document must be produced after each meeting of the Advisory Board, Executive Board, General assembly meetings and other meetings where the importance or a need to deliver and keeping Minutes of Meetings is considered by partner (see ch. 6.3.6 and ch. 6.5 of the CA and ch. 4.3.1 of the D9.1 Project Quality Handbook), shared for review with other partners and filed in a repository (consortium MS Teams, relevant WP file as per Findability requirement according to GA, ch. 1.2.7, Table 11). Risks are then transferred to another formal document Risks register, which is also kept in the same repository. Another measure to keep consortium members aware of the importance of following the situation with potential problems with data privacy and security as well as of non-compliance is the compulsory documentation of any (critical) risks in continuous reporting (Article 21 in the GA).

If the recording of meetings is needed that is related to the work on tasks, consent to the recording is required from participants either by expressing it in the chat (online meetings) in the form of disagreement written in the chat, if somebody does not agree or by refusing it with a signature in a formal document which is the part of the Attendance *List* (Annex 3 of this deliverable). If the consent is not given, no recording is made. Existing recordings are kept in the consortium repository (MS Teams). Consent will be used also in case when working with employees and/or end-users of products (if necessary).

- *Data storage, preservation, back up and retrieval* - establishing efficient and scalable mechanisms for storing and retrieving data. This involves selecting appropriate storage infrastructure and technologies for ensuring data durability and availability, optimizing data access performance, and implementing data archiving and backup strategies. This includes selecting storage solutions that meet the data's specific requirements in terms of capacity, performance, and redundancy, as well as establishing regular backup and disaster recovery procedures. This also means planning for the long-term preservation and accessibility of the data beyond the project's duration. This may involve considerations such as data archiving, data format migration, and metadata preservation to ensure that the data remains usable and accessible over time (Van den Eunden et al, 2011, Ashiq et al, 2022).

As in the previous points, most of the issues have been discussed and ensured before the **project DiCiM** had started and are included in the GA (chapter 1.2.7, part B). More information is in chapter 4 in this deliverable.

- *Data collaboration, sharing and long-term access* - promoting collaboration and knowledge sharing through effective data management practices, identifying and defining the mechanisms and policies for sharing and providing access to the data. This includes facilitating data sharing among different departments or teams, implementing data governance frameworks, and fostering a culture of data-driven collaboration among project team members and with other relevant partners if interested in, specifying who can access the data, under what conditions, and any necessary

Funded by the European Union

agreements or licenses. The objective is to facilitate data sharing among collaborators, researchers, or the wider community while respecting data privacy and security (Sukumar and Ferrell, 2013; Desai et al, 2016).

With the **DiCiM project** access rights (also in the long-term perspective) have been already mentioned in the issue related to the data security, privacy and compliance and will be dealt with in chapter 4. Governance is outlined in the following point and in chapter 6.2. Facilitation of data sharing together with the policy and mechanisms for data sharing as well as fostering of the appropriate and proper culture for data sharing and data collaboration is an integral part of the work on the tasks within the individual work packages and core of the project. Potential collaboration with partners' projects and sharing the data which are not confidential and sensitive will be discussed and agreed to by WP leaders and project coordinator when actual collaboration starts. Confidentiality of data and records will be kept 5 years after the final payment from granting authority is realized (chapter 6 Other of Data Sheet – General data, GA). The aforementioned allocated PIDs will enable sharing of data.

- *Data resource planning and cost optimization* - identifying the resources required to effectively implement the data management plan, including personnel, infrastructure, tools, and budget. This includes considering the costs associated with data storage, security measures, data curation, and any necessary training or support. Optimizing the cost of data management activities, including storage, processing, and maintenance means identifying opportunities for cost reduction, such as data deduplication, archival strategies, or cloud-based storage solutions (Goodhue et al, 1988; Eppler and Helfert, 2004; Haug et al, 2011; Otto, 2015; Grande et al, 2020).

Resources for data management for the DiCiM project have been identified and planned already for the proposal. Ensuring availability of resources, providing them and spending them in accordance with good and sound management is the task of all consortium members, more specifically of WP leaders and the coordinator. In particular, non-compliance with the requirements for the use of financial resources relating to data management is against the rules stated by the granting authority and included in the GA and mechanisms of resource utilization control must be applied, especially through continuous budget spending controls and through compulsory reporting. The use of financial resources is closely linked to the use of other resources.

Funded by
the European Union

3. Data summary

Most of the points concerning data described below will be monitored throughout the project realization by the coordinator of the project as the part of the updating this IDMP in the form of table which is available in the Annex 1. As mentioned above DMP is a living document to be adapted if and when needed and supplemented by new information if it arises. Table in Annex 1 will gather data about types and formats of data, names of datasets, data source/origin, sensitivity of data and other relevant issues which be changed or new and their knowledge is important for making data findable, accessible, interoperable and able to re-use.

3.1. Purpose of data

DiCiM project will collect and generate product, process and socio-economic data related to the Circular Economy, more specifically data coming from tracking and tracing product forward and reverse flows and product condition within the target of interest in the automotive, electronics and whitegoods sectors. Data will serve for further study of the respected area, for gaining insights into the challenges and opportunities of data digitalization for the circular economy purpose and for benchmarking for other industries and sectors.

3.2. Expected users of data and datasets

Open datasets could be relevant and useful for researchers from the consortium, researchers beyond consortium for further study and research, analysis – if possible and as mentioned above – for benchmarking (industrial and sectoral, time, technology etc.) Second group of potential interested parties are industrial partners – again for the insights into the new solutions, for potential application or further development as well as research. Also other players from industries could learn and re-use some results which will be openly accessible. The same is with the R&D organizations and firms. Academicians for the purpose of education are another potential user of the findings as well as students. Finally public authorities who play and may play important roles in promoting project and its results as well as knowledge growth of the digitalization of circular economy processes, facilitating application of results in practice and enabling braking barriers and coping with various challenges concerning circular economy in general as well as digitalization of the industrial and different business processes. Among them policies makers act as a very significant group.

3.3. Types and categories of data

DiCiM project research data can be divided into several **types:**

Main research data generated by demonstrations, more specifically during technologies development, deployment, testing, validation and training are:

- product,
- process and
- socio-economic data.

Funded by the European Union

After analyses, research data will exist in the form of:

- article preprints,
- peer-reviewed articles in scholarly journals,
- articles (papers) in conference proceedings,
- monographs,
- patents, and
- research data as data underlying publications, curated data and/or raw data.

There will be two main **categories of research data**:

a) *manually collected* – data from co-creation workshops with demonstrators, from the interviews with demonstrators beyond the workshops, formal and informal meetings, literature reviews, existing data that will be re-used in the project, conferences, and other events etc., which are relevant for solutions of the project tasks

b) *automatically collected* – data from the developed and applied technologies and digital open access platform implementation and demonstration. All of these data come from production, logistics (forward, reverse and in-house) and customer product use processes, more specifically real time data from the processes of product and parts tracking, tracing, and condition monitoring before the products leave manufacturing and warehousing processes and in the use phase by customers (where also repair services could be realized). After the return of products, data flow from the processes of collection, inspection, sorting, disassembly/dismantling, testing and repair, reassembly, refurbishing, remanufacturing and/or potentially also from recycling.

Part of the research data could be anonymised, while some of them could not be and must be stored and protected only for the internal use of the demonstrators with controlled access. Part of the processed non-anonymisable data will be included in the reports marked as sensitive (SEN). Anonymisable data should become part of the open science policy and will be published according to the rules of the GA and CA.

There are several forms of publishing these analysed and processed anonymisable data, as for instance:

A) in the form of deliverables which are public (PU);

B) in the form of theses, dissertations;

C) in the form of scientific articles;

D) in the form of news, presentations at events;

E) in the form of the educational and training materials.

3.4. Sources/origins of data

Most of the data will be generated from the demonstrators as a result of the co-creation workshops to identify business, technical and legal requirements etc. Futher data will be developed as part of evaluation of demonstrators: when testing and evaluating digital circular support solutions, evaluation of training activities. A second source of data is the existing published knowledge, experiences and best practices from secondary sources.

Funded by the European Union

3.5. Formats of data

Different formats of data will be generated, used and shared within individual WPs and Tasks.

The following list contains the most widely accepted formats for data which will be stored and shared in the DiCiM project, such as:

- Documents/Reports/Publications: .PDF (different available types) txt, .docx
- Spreadsheets: .xslx
- Databases: .cvs
- Data interchange formats: .xml, .json
- Audio files. .mp3, .wav, .wma, .ra
- Pictures: jpg, png
- Video: avi, flv, mov, mp4, wmv

Other formats will be added by partners into the table that will be used for monitoring data related information (available in the Annex 1).

3.6. Dates related to dissemination and exploitation of data and research results

For planning dissemination activities agreed dates are important. Agreed rules and dates are included in the GA and CA. The plan for dissemination and exploitation is part of the D8.2 Communication and dissemination plan (M6).

The following Table 1 provides an overview of dates binding for dissemination and exploitation activities:

Table 1: Dissemination dates:

Dissemination and exploitation type	What and who	To whom (announced)/ where (to upload)	Date	Comment
result	notice - dissemination - beneficiary	other beneficiaries	at least 15 days advance	Any other beneficiary may object within 15 days of receiving notification (unless agreed otherwise), if it can show that its legitimate interests in relation to the results or background would be significantly harmed
planned publication	prior notice - author(s)	other internal parties	45 calendar days	Objecting party can request a publication delay of not more than 90 calendar days from the time it raises such an objection. After 90
	Objection to planned	Coordinator and internal party(ies)	Within 30 calendar days	

Funded by the European Union

	publication – objecting party	proposing the dissemination	after receipt of the notice	calendar days the publication is permitted, provided that the objections of the objecting Party have been addressed
final version of article or conference proceeding	posting	consortium repository	immediately	
open access to the deposited publication	ensuring	consortium repository	Within 6 months after publication	
granting non-exclusive licences to third parties to exploit the jointly-owned results	notice - joint-owner	another joint-owner	45 days (at least)	
possible standardisation	Information – relevant beneficiary	Granting authority	upon to 4 years after the action	
transfer of the ownership	information	other beneficiaries with access rights of the transfer	at least 45 days in advance	The beneficiaries may object within 30 days of receiving notification (or less if agreed in writing), if they can show that the transfer would adversely affect their access rights

Funded by the European Union

4. FAIR data

4.1. *Making data findable, including provisions for metadata*

Uniform, clear and concise labelling of data is essential for data (and datasets findability) as well as to use channels or media that are widely accepted and easily accessed. DiCiM projects strictly adheres to the Open access policy and several measures have been taken into consideration already during the proposal preparation.

The first is decision making about the right repositories – this issue is addressed in chapter 4.2.

The second is application of naming conventions for data and datasets as well as other research outputs description – this is elaborated in chapter 4.1.1.

Finally, internationally accepted tools for data as well as researchers identification are outlined in chapter 4.1.2.

Findability aspects are included in the GA, ch. 1.2.7. This chapter covers naming conventions for the repository (MS Teams) for both project documents and for meeting minutes.

4.1.1. Naming conventions

Data findability and searchability can be enhanced following a consistent set of naming conventions. For DiCiM datasets and documents a consistent set of naming conventions includes with some variations for administrative documents (e.g. Minutes of Meetings, communication materials, templates etc.):

The most typical naming – especially for the internal purpose:

- the document type designation and, if relevant, the number of document (e.g. in case of deliverables: Dx.x_Deliverable)
- version of the document (either only number: 1 or 01 or v01)

This DMP also recommends the following rules for file naming:

1. for data set file(s)

PROJECT ACRONYM_TaskNumber_Coverage or other content specifications_Date(YYYYMMDD)_VersionNumber.fileExtention

2. for README file(s)
PROJECT ACRONYM_TaskNumber_Coverage or other content specifications_Date(YYYYMMDD)_VersionNumber_README.fileExtention

For Zenodo, the metadata associated with each published data set will by default be as follows:

- Digital Object/Author(s) Identifiers – see also chapter 4.1.2
- Title of the document
- The document type designation and, if relevant, the number of document (e.g. in case of deliverables: Dx.x_Deliverable)

Funded by
the European Union

- Acronym of the project name
- Long project name
- Number of the project
- Granting authority
- Version number
- Author(s) name(s) – if relevant
- Keywords
- Abstract/description
- Language
- Access and licensing info – if relevant.

4.1.2. *Digital Object and Author Identifier*

When possible, Digital Object (DOI) and/or Author Identifier (ORCID) will be used to identify content, connection to the project and to authors. These identifiers provide a persistent link to their locations on the internet.

4.2. Making data accessible

Access rights to results including software are contained in the chapter 9 of the CA and in Article 16 of the GA. There will be three main channels for open access research data and research results:

1. Non-sensitive and non-confidential data will be available through the project website. CHX is responsible for uploading such documents and making them accessible for the time limit set and under the conditions and requirements and status given to the different types of documents stated in the GA. The Coordinator´s role is to control correct treatment of documents.

2. These types of data will be accessible (in the form of data sets and scientific publications) also in the repository Zenodo, which enables FAIR principles. In this repository data are given a persistent digital object identifier (DOI) and objects are linked also to the authors via ORCID numbers. Clear designation to the project is also enabled.

3. The third channel for both open and restricted access is the partners' private repository.

If throughout the project life consortium members will consider using other repositories (e.g. European Open Science Cloud (EOSC), the European Data Infrastructure (EDI) and the Open Research Europe publishing platform as already planned in the project proposal and contained also in the GA), the verification of suitability must precede the proposal and discussion between consortium members. The Executive Board has the right to decide based on the evaluation of facts.

Access to the data which are sensitive and confidential could be given only under the conditions set out in the GA and CA.

The plan for the open access dissemination is part of the Deliverable 8.2 Communication and dissemination plan, as already mentioned.

Funded by the European Union

4.3. Making data interoperable

All data sets will be described using standard descriptive metadata, in order to ensure metadata interoperability for indexing and discoverability. Data generators and collectors are responsible for this activity. Where possible all shareable data will be adapted from proprietary formats to well-known and documented open formats (e.g. xml, csv or txt – see also chapter 4.3). This interoperability approach allows data exchange and re-use between different researchers, teams, consortium partners if involved in research, as well as the other interested external parties.

In case specific software is used during and for data processing, full explanation and instructions will be included in the deposited documentation.

According to the GA, Part B metadata vocabularies, standards and methodologies according to the purpose will be developed by the relevant researchers in the following areas (for some details see also chapter 4.1.1 and 4.1.2):

(i) Descriptive metadata to help users discover and identify a resource (e.g., Title, Abstract, Author, and Keywords);

(ii) Administrative metadata to manage an information resource (e.g., provenance, processing, and rights information);

(iii) Structural metadata which describe the relationship between parts of an information resource, especially digital resources, which often consist of multiple files;

(iv) Technical metadata to document technical attributes of digital objects or resources;

(v) Preservation metadata to support and document the long-term digital preservation of an information resource or digital object.

4.4. Increase data re-use

DiCiM project aims at making use of as much both existing previous research effort either from the consortium members as well as of the existing literature and knowledge as possible. The same is with the results of project as such for the external parties if possible.

Re-use of existing data and information is considered as the part of several Tasks, more specifically of the Tasks 1.1, 1.2 and 1.3, 2.1, 3.1 However, flows of generated and analysed data for the purpose of re-use among the work packages and tasks create the core of the project as the packages and tasks are more or less interlinked.

All issued documentation generated by consortium members will include basic information about the data that allow for its correct interpretation for internal reuse and if not sensitive data, also for use by other researchers (e.g., README file, README tab, Data Dictionary, Codebook, Commented Code, Lab Notebooks, as applicable). Decision making about the form will be done by the WP or Task leaders.

Results in the form of data, datasets, software or other expected results which are eligible for sharing externally and are protected by the terms of the IPR according to the terms of the GA and CA will be accompanied by a data license that details the permissions associated with the use of that dataset. The licenses for each dataset will be stored in their respective repository, where they will be found in the respective dataset's README and metadata file. Template for dataset README file is in the Annex 2.

Funded by
the European Union

Funded by
the European Union

5. Other research outputs

Among planned research outputs the following belong:

- software
- open access digital platform
- machine learning algorithms
- augmented reality applications
- efficient product and part recovery mechanism
- appliances repairing data management
- condition monitoring solution
- contents and materials for education
- models and KPIs for performance evaluations
- standard(s)

All research outputs have been planned as part of data generation and collection as the objectives of the project and as the part of the exploitation strategy and specific processes related to FAIR principles are established and are introduced in the GA, Part B and relevant chapters of the GA and CA.

Funded by
the European Union

6. Allocation of resources

6.1. Costs making data and other research outputs FAIR

The estimation of the resources for data processes and data management and making data FAIR were already considered when drafting the budget for the project proposal before being submitted to the European Commission. Purchase costs which cover also costs for data management (together with open access publishing costs) are included in specific Table of Part B of the GA (pp. 32 and 33).

If any changes which will be relevant for the evaluation occur during the project duration and which would need adaptation of resource utilization and flows, they shall be discussed and agreed by the Executive Board members and/or by General assembly (see also chapter 4.2 Planning of the D9.1 Project Quality Handbook).

6.2. Data management responsibilities

Data management responsibilities (human resources management) are and will be distributed according to the Data Governance. **Governance structure** for data security contains several roles and levels of responsibility. The coordinator has the biggest responsibility for ensuring that data are managed in a secure way. There are also the main **Data controller** (in case of the personal data collection and processing). WP leaders are responsible for data security within packages and individual tasks. At the task level, they check the correctness of data security tasks performed by task leaders. Both coordinator and WP leaders work as data controllers in case of handling personal data and as **Data processors** performing data-related processes. Except for these two roles, every consortium member works as the data processor and is responsible for data security within his/her specific task. Task leaders and WP leaders control the quality of work on data security of data processors.

In case of the personal data collection there is also a role of the **Data contributors**. These are participants of research data collection from individual persons. More to the governance structure in chapter 8 and “Who” part.

Also, subcontractors could participate in the research. Their responsibilities and responsibilities of the beneficiaries who involve subcontractors are regulated by the chapter 9.3 of the GA.

Funded by
the European Union

7. Data security

Data security issues are part of Article 13 in terms of confidentiality and sensitivity, in term of data protection part of Article 15 and indirectly also as a part of Article 16 – IPR, of Annex 5, of the chapter 1.2.7 of the Part B of the GA and chapter 10 of the CA. Initial IPR registry has been created at the beginning of the project and it is available on p. 30 of the Part B, of the GA, Table 21.

Article 16 of the Annex 5 of the GA establishes the obligation to protect results of the research stating the following:
"Beneficiaries which have received funding under the grant must adequately protect their results — for an appropriate period and with appropriate territorial coverage — if protection is possible and justified, taking into account all relevant considerations, including the prospects for commercial exploitation, the legitimate interests of the other beneficiaries and any other legitimate interests."

To monitor compliance with this obligation the following Table 2 will be used. It will serve as the IPR register (see also information in chapter 8 "How" on IPR), but according to agreement of the Executive Board members it could be used for any relevant result. More information is available in chapter 8, part "How" concerning IPR register in this IDMP:

Table 2: IPR register

WP	Protected result (software, technology, methodology…)	Method of protection (trademarks, patents, copyright and transfer and licensing agreements…)	Owner	Status of protection	Dissemination	Protection period	Territory
1							
2							
3							
4							
5							
6							
7							
8							
9							

Data security measures can be divided into those relating to internal and those relating to external data-related communications:

a) internal communication:

What, who, where, when and how:

There is a need to secure data by and among members of the consortium. For the **internal communication** data are stored and archived in the agreed and structured database in the MS Teams environment. Only members with entry rights are able to access and work with data.

Funded by the European Union

Deliverables which contain confidential and sensitive data are specifically tagged in the database to store them, which acts in part as a warning signal for handling the data they contain. MS Teams environment enables to follow some processes with data (who and when uploads the document, who changes/adapts it) which also improves security of data (see chapter 4.3 Internal Communication of D9.1 Project quality handbook). MS Teams is considered to be a highly trusted platform for keeping and sharing confidential and sensitive data.

Not all functions are utilised on the date of this deliverable release. However, the plan is to organize a meeting with MS Teams experts to discover and apply more security measures during M9 so the first deliverables which are tagged as SEN will have the highest protection. Coordinating team will organize this meeting and information as well as concrete measures will be presented and discussed with WP leaders and demonstrators during September 2023 and if agreed, they will be implemented ASAP after the presentation. Relevant information and results will be included in the updated version of the IDMP, stored in the repository (MS Teams) and shared with partners.

Consortium members will also store their data and datasets in their own repositories. For the assurance of the data security the WP designated person of each partner is responsible. List of designated persons will be prepared and stored in the project consortium repository in September 2023 and updated upon the request of partners by the coordinator.

b) external communication:

What, who, where, when and how:

Zenodo platform is chosen by consortium partners as one of two external channels of storing the data which are not confidential and sensitive. The second one is the DiCiM project website. Responsibility for data security for the second case is held by Crowdhelix. WP leads will share relevant data, datasets and/or documents with Crowdhelix who will upload and keep them on the web repository. For Zenodo, every WP leader is responsible to upload and properly identify document which will be accessed according to the open access policy. Zenodo is also the repository where articles, conference papers and theses will be available and uploaded either by the authors themselves or by the WP leaders. The coordinator´s role will be to control the status and if the document is missing to ask relevant person to upload missing document with the proper identification. Plan for such publishing activities and report of existing publishing activities will be part of the 6-months report during the General assemblies and also will be included in the Communication and dissemination tracker held by Crowdhelix (see also D8.2).

As stated in the GA, Part B, chapter 1.2.7, relevant data will be placed in open repositories after a grace period (which means 14 days after the conclusion is done by the generator of data that data are ready for publishing) for the consortium members to properly curate and assess whether some results are sensitive in nature, given the strategic importance of the production environments and supply chains.

Funded by
the European Union

8. Ethics

Ethics of research and data management is covered in Article 14 of the GA and specific ethics rules set out in Annex 5, then chapter 1.2.7 – Table 11 and chapter 4 of Part B of the GA. The DiCiM project involves human participants, but it is not planned to process any personal data in terms of research itself (see Ethics Issue Table, p. 35 of Part B of the GA). If this will change throughout the project realization, discussion on potential impacts should be start immediately upon the detection of a need for such change between relevant WP leader, coordinator and members of the Executive Board.

Ethics matters related to personal data are content of the Ethics self-assessment rules in Part B of the GA.

Who:

Primary responsibility for monitoring and evaluating ethical aspects of data management (especially of data privacy) together with the social impact of the project lies with *the project coordinator* who is also a leader of the WP dedicated – besides other issues — to data management, specifically in the context of Tasks 9.2, 9.3 and 9.4. The coordinator also acts as the main Data controller, however he/she works also as the data processor.

Ethics matters are also a responsibility of every WP leader in the scope and content of the specific package. If there are also other partners in WP who lead specific task within the package, it is again the WP leader who is responsible for non-existence of any ethical issues concerning the task realization. Both WP leaders and Task leaders act as data controller and data processors.

At the lowest level of responsibility for ethical matters of data management are all members of the consortium for the tasks assigned to them by WP and Tasks leaders. Again, also at this level these people work as the Data controller and data processors. This means there is a chain of commands within the hierarchical management control function.

According to Article 9.2 of the GA if project consortium members hire subcontractors, all their contractual obligations – including ethical aspects — will apply also to subcontractors.

What:

Potential ethics or legal issues may arise in relation to the sharing or dissemination of data to persons without the right to obtain and use that data or in the case of new legal requirements on data management emerge but the assessment of these issues could not be included in the proposal of the project and the GA and CA. According to the Article 14 of the Annex 5 and concerning ethics and legal requirements of data management beneficiaries must pay particular attention to the right to privacy and the right to the protection of personal data. They also must respect the fundamental principle of research integrity. This specifically means:

- reliability in ensuring the quality of research reflected in the design, the methodology, the analysis and the use of resources;
- honesty in developing, undertaking, reviewing, reporting and communicating research in a transparent, fair and unbiased way;
- respect for colleagues, research participants, society, ecosystems, cultural heritage and the environment;

Funded by the European Union

- accountability for the research from idea to publication, for its management and organisation, for training, supervision and mentoring, and for its wider impacts and means that beneficiaries must ensure that persons carrying out research tasks follow the good research practices including ensuring, where possible, openness, reproducibility and traceability and refrain from the research integrity violations described in the Code[1].

Personal data: as mentioned above no personal data should be collected and processed during the project as research data. However, if such situation emerges, there are the GDPR compliance measures taken in the GA (see Articles and chapters introduced above in this part of the Deliverable, more specifically Article 15. 1 and 15. 2 of the GA).

IPR data: IPR are included in Article 16 of the GA (provision of and access right to background information, ownership of the results and rights of use of the granting authority of research data). Annex 5 of the GA contains specific rules on IPR, results and background.

Confidential (sensitive) data: are covered in Article 13 of the GA and set out the conditions for working with such data — the period during which these data are to be managed as confidential and sensitive, purpose for and the conditions under which such information may be disclosed to the employees and partners of the beneficiaries and by granting authority

When:
Ethical data management issues must be taken into account throughout the project and for a certain period of time — specified in the GA – also after the end of the project. Special data related to the data management after the project are agreed among consortium members and with the granting authority and are introduced in Data Sheet, point 6 of the GA. For data management time for data confidentiality and record keeping is 5 years after the final payment will be realized.

Annex 5, Article 13 states specific requirements that includes also „time“ in case of an action task raising ethical issues. Before starting such an action *„the beneficiaries must have obtained all approvals or other mandatory documents needed for implementing the task, notably from any (national or local) ethics committee or other bodies such as data protection authorities*.“

Where:
Ethics requirements and rules on data management have to be applied in any country, in any organization and in any situation where DiCiM research is realized, data management processes provided, communicated and disseminated and research results are exploited. In case of needed and justified data transfer across borders for exploitation the Data controllers are solely responsible for adhering to the legal requirements

How (and who and when):
For *personal data* (see also text above) management all regulations on General Data Protection (GDPR) will be adhered to. Informed consent forms for participation in research and for processing data will be included in each data collection task dealing with personal data. Participants have to sign informed consent with explicit information (given in the information

[1] European Code of Conduct for Research Integrity

Funded by the European Union

sheet) before the data collection. Beneficiary who will collect the data (data collector and data controller in one unified role) is responsible for informing participants about the future use and processes of their data, of the purpose and methods of collection in the way appropriate for the participants in the research.

After the collection of data is completed, collected data must be anonymized and personal and non-personal data separated by the data processor. This means that all materials that could lead to an identification of the person (e.g., informed consent, names/codes list used for pseudonymization) will be stored separately from research data and research data will be anonymized and aggregated according to the purpose of the analysis.

The research data will be stored on a separate file and do not contain any personal data. Association between research participants personal data and research data will be managed from the security and privacy issues by the beneficiary who collects the data on his/her responsibility. If the participants subsequently make a request to withdraw consent, it must be granted and all data deleted. This option must be clearly described in the informed consent form.

If needed, the form for informed consent and information sheet (included in the single piece of paper) will be prepared by Coordinator (main Data controller) and agreed by the Executive Board. So far (June 2023) there is only reduced consent for the data collectors and data processors related to photos taken from co-creation sessions and from the on-site visits and for recording the sessions.

IPR strategy is realized according to the aims and measures contained in chapter 2.2.3, Part B of the GA. Its updating will follow new requirements based on the results of the processes under the Communication adopted by Commission in November 2020[2]. C-ECO (Task 8.4 IPR Management leader) upon the supervision of the Executive Board (see ch. 2.2.3 of the GA, p. 30, Part B concerning responsibility of the Executive Board) will maintain an IPR register throughout the lifetime of the project (see Table 2 for IPR register in chapter 7). This register, although the main activities will be realized due M25 – 48, will be regularly updated and distributed to all partners (see ch. 2.2.3 of the GA, p. 30, Part B) by the C-ECO via MS Teams messaging and emails. The initial version of the register will be released in August 2023. Initial agreement on IP and use rights has been agreed by consortium members before proposal submission and it is included in chapter 2.2.3, Part B of the GA.

[2] COM(2020) 760 - Making the most of the EU’s innovative potential – An intellectual property action plan to support the EU’s recovery and resilience available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52020DC0760

Funded by the European Union

9. Conclusions and next steps

This deliverable describes the initial plan of data management issues. As a living document the plan will be updated continuously. Several steps will be taken for updating along the project lifecycle as it is shown at the Table 3 which will document for every year of the project the *when, what, who, how* and *where*. This table serves the management of the project as a part of a continuous reporting and will be filled by the coordinator and controlled by WP and Task leaders.

Table 3: Data management overview

2023 Data management processes	WP Task Who	When	What and how	Where (databases, deliverables etc.)
Data planning and decision making	WP1, Task 1.2 (and 1.1)	January-February	Protocols, memo	
Data generation				
Data collection				
Data formation				
Data analysis				
Data quality verification				
Data approval				
Data integration				
Data storage and preservation				
Data protection				
Data use				
Data sharing				
Data licensing				

After the project formally ends, the data owners will continue to manage certain processes according to conditions and requirements of the GA.

Funded by
the European Union

10. References

Al-Badi, A., Tarhini, A., & Khan, A. I. (2018). Exploring big data governance frameworks. *Procedia computer science*, *141*, 271-277.

Alhassan, I., Sammon, D., & Daly, M. (2016). Data governance activities: an analysis of the literature. *Journal of Decision Systems*, *25*(sup1), 64-75.

Ashiq, M., Usmani, M. H., & Naeem, M. (2022). A systematic literature review on research data management practices and services. *Global Knowledge, Memory and Communication*, *71*(8/9), 649-671.

COM(2020) 760 - Making the most of the EU's innovative potential – An intellectual property action plan to support the EU's recovery and resilience available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52020DC0760

Desai, T., Ritchie, F., & Welpton, R. (2016). Five Safes: designing data access for research. *Economics Working Paper Series*, *1601*, 28.

Eppler, M., & Helfert, M. (2004, November). A classification and analysis of data quality costs. In *International Conference on Information Quality* (pp. 311-325). Cambridge: MIT.

Gao, J., Xie, C., & Tao, C. (2016, March). Big data validation and quality assurance—issuses, challenges, and needs. In *2016 IEEE symposium on service-oriented system engineering (SOSE)* (pp. 433-441). IEEE.

Georgiadis, G., & Poels, G. (2021). Enterprise architecture management as a solution for addressing general data protection regulation requirements in a big data context: a systematic mapping study. *Information Systems and e-Business Management*, *19*, 313-362.

Goodhue, D. L., Quillard, J. A., & Rockart, J. F. (1988). Managing the data resource: a contingency perspective. *MIS quarterly*, 373-392.

Grande, D., Machado, J., Petzold, B., & Roth, M. (2020). Reducing data costs without jeopardizing growth. *McKinsey Digital,* *https://www.mckinsey.com.br/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Reducing%20data%20costs%20without%20jeopardizing%20growth/reducing-data-costs-not-jeopardizing-growth.pdf*

Grover, V., Chiang, R. H., Liang, T. P., & Zhang, D. (2018). Creating strategic business value from big data analytics: A research framework. *Journal of management information systems*, *35*(2), 388-423.

Haug, A., Zachariassen, F., & Van Liempd, D. (2011). The costs of poor data quality. *Journal of Industrial Engineering and Management (JIEM)*, *4*(2), 168-193.

Mahanti, R., & Mahanti, R. (2021). *Data governance and compliance* (pp. 109-153). Springer Singapore.

Otto, B. (2015). Quality and value of the data resource in large enterprises. *Information Systems Management*, *32*(3), 234-251.

Phillips-Wren, G., Iyer, L. S., Kulkarni, U., & Ariyachandra, T. (2015). Business analytics in the context of big data: A roadmap for research. *Communications of the Association for Information Systems*, *37*(1), 23.

Funded by
the European Union

Rahul, K., & Banyal, R. K. (2020). Data life cycle management in big data analytics. *Procedia Computer Science*, *173*, 364-371.

Schäfer, F., Gebauer, H., Gröger, C., Gassmann, O., & Wortmann, F. (2022). Data-driven business and data privacy: Challenges and measures for product companies. *Business Horizons*.

Sinaeepourfard, A., Garcia, J., Masip-Bruin, X., & Marín-Torder, E. (2016, December). Towards a comprehensive data lifecycle model for big data environments. In *Proceedings of the 3rd IEEE/ACM International Conference on Big Data Computing, Applications and Technologies* (pp. 100-106).

Sukumar, S. R., & Ferrell, R. K. (2013). 'Big Data'collaboration: Exploring, recording and sharing enterprise knowledge. *Information Services & Use*, *33*(3-4), 257-270.

Strasser, C., Cook, R., Michener, W., & Budden, A. (2012). Primer on Data Management: What you always wanted to know.

Van den Eynden, V., Corti, L., Woollard, M., Bishop, L., & Horton, L. (2011). Managing and sharing data; a best practice guide for researchers.

Walls, C., & Barnard, B. (2020). Success factors of Big Data to achieve organizational performance: Theoretical perspectives. *Expert Journal of Business and Management*, *8*(1).

Wang, Y., Hulstijn, J., & Tan, Y. H. (2016). Data quality assurance in international supply chains: an application of the value cycle approach to customs reporting. *International Journal of Advanced Logistics*, *5*(2), 76-85.

Funded by
the European Union

11. Annex 1 Data management sheet

Data management sheet

Types of data: experimental, observational, images, text, numerical, other – please, specify

****Format of data:**
Documents/Reports/Publications: .PDF/A, txt, doc/docx
Spreadsheets: .xls/.xslx
Databases: .cvs
Audio files. .mp3, .wav, .wma, .ra
Pictures: jpg, png
Video: avi, flv, mov, mp4, wmv
Other: please, specify

***** According to **chapter 10.1 of the Consortium agreement a *"Confidential Information*"** means all information, for example data, drawings, 3D models, drafts, sketches, plans, descriptions, specifications, measurement and test results, testing methods, calculations, experience, processes, samples, molds, installations, tools, patent applications not yet published, know-how, commercial documents, marketing strategies, purchasing addresses, cooperation partners, names of customers, hardware and software configurations, access codewords or software, regardless of its physical form or characteristics disclosed in connection with the Action, that is marked as "confidential", and which constitutes trade secrets within the meaning of Directive (EU) 2016/943 because (1) it is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question, (2) it has commercial value because it is secret and (3) it has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.

******Classified information (PROBABLY NONE IN DiCiM – according to Grant Agreement) but PLEASE, READ THIS MATERIAL: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/classification-of-information-in-he-projects_he_en.pdf and Article 13.2 and Annex 5 of Grant Agreement*

Items	WP1			Comments and potential risks of data management
	Task 1.1	*Task 1.2*	*Task 1.3*	
Name of dataset	Technical requirement specifications	Business requirement specifications	Legal requirement specifications	
Type of data*	Text, audio recordings	Text, video recordings, audio recordings	Text, audio recordings	
Description of data	Interviews, group	Interviews, group discussions, presentations	Interviews, group discussions, presentations	

Funded by the European Union

	discussions, presentations			
Source/origin of data	Co-creation workshops with demos	Co-creation workshops with demos; online interviews, internal documents, literature review	Review of scientific publications, reports and legislative documentations; interviews with the employees of legal departments of demos	
Format of data**	PDF, docx, .wav, .mp4, ppt	PDF, docx, .wav, .mp4, ppt	PDF, docx, .wav, .mp4, ppt	
Personal data (1 – yes, 0 – no)	0	0	0	
Responsible data controller	KTH	MUNI	KTH	
Confidential information (1 – yes, 0 – no)***	1	1	0	
Method(s) of access restriction to confidential information by partner	Internal Teams team	Internal Teams team	Internal Teams team	
Dissemination level (sensitive - SEN, public - PU)	SEN	SEN	PU	
Deliverable	D1.1	D1.2	D1.3	
Classified information* (1 – yes, 0 – no)***				

Items	**WP2**			**Comments and potential risks of data management**
	Task 2.1	***Task 2.2***	***Task 2.3***	
Name of dataset	Baseline of current key technology features for support solutions	Target technologies development and adaptation requirements	Technology deployment, demonstration, and testing plan	
Type of data*	Text with images	Text with images	Text with images	
Description of data				
Source/origin of data	Literature review and interviews with demos and technology providers	Demos/users	Common planning with all partners of the consortia	

Funded by the European Union

Format of data**	.PDF/A, doc/docx, jpg, png	.PDF/A, doc/docx, jpg, png	.PDF/A, doc/docx, jpg, png	
Personal data (1 – yes, 0 – no)	0	0	0	
Responsible data controller	TUC	ULFS	TUC	
Confidential information (1 – yes, 0 – no)***	0	Not Sure	Not Sure	
Method(s) of access restriction to confidential information by partner	N/A	N/A	N/A	
Dissemination level (sensitive - SEN, public - PU)	PU	SEN	SEN	
Deliverable	D2.1	D2.2	D2.3	
Classified information* (1 – yes, 0 – no)***	0	0	0	

Items	**WP3**				**Comments and potential risks of data management**
	Task 3.1	***Task 3.2***	***Task 3.3***	***Task 3.4***	
Name of dataset	Open access digital platform technology requirements and specifications	Solution design of the Open access digital platform	Development of open access circular information management platform	Development of extended automotive part data management platform	
Type of data*	text	text	text		
Description of data					
Source/origin of data	Literature review and interviews with demos and technology providers	Demos/users			
Format of data**					
Personal data (1 – yes, 0 – no)					
Responsible data controller					
Confidential information (1 – yes, 0 – no)***					

Method(s) of access restriction to confidential information by partner					
Dissemination level (sensitive - SEN, public - PU)	SEN	SEN	PU	SEN	
Deliverable	D3.1	D3.2	D3.3	D3.4	
Classified information* (1 – yes, 0 – no)***					

Items	**WP4**					**Comments and potential risks of data management**
	Task 4.1	***Task 4.2***	***Task 4.3***	***Task 4.4***	**Task 4.5**	
Name of dataset	Report on IoT tracking and tracing capability of washing machines and printers	Report on IoT for condition monitoring of washing machines and printers	Report on AI for decision making	Report on image processing technology development	Report on AR-application to support disassembly and value recovery	
Type of data*	Text, graphs, pictures, tables	text	text	Notes,text, graphs, images, videos, reports and all related to the modelling and Task T4.4	Text, graphs, pictures, tables, videos, 3D-Models	
Description of data				Models, reports, images, demos and specific data from T4.4.		
Source/origin of data	Data from IoT tracking and tracing and interview			Data from reviews, Internal IRIS developments and modelling, including results and validations	Data provided by C-ECO and Gorenje. Data provided by IDENER, ULFS, IRIS	

Funded by the European Union

	s with demos					
Format of data*	.PDF/A, doc/doc, jpg, png			Documents/Reports/ Publications: .PDF/A, txt, doc/docx Spreadsheets: .xls/.xslx Databases: .cvs Audio files. .mp3, .wav, .wma, .ra Pictures: jpg, png Video: avi, flv, mov, mp4, wmv Other: 3D-Models in fbx, obj, stl	Documents/Reports/ Publications: .PDF/A, txt, doc/docx Spreadsheets: .xls/.xslx Databases: .cvs Audio files. .mp3, .wav, .wma, .ra Pictures: jpg, png Video: avi, flv, mov, mp4, wmv Other: 3D-Models in fbx, obj, stl	
Personal data (1 – yes, 0 – no)	0			0	Maybe, I do not know yet	
Responsible data controller	GORENJE	Lexmark		IRIS	TUC	
Confidential information (1 – yes, 0 – no)***	1	1		1	1	
Method(s) of access restriction to confidential information by partner	Each partner will protect the data's confidentiality.			Each partner will protect the data's confidentiality, through access regulation, VPN, Back-UPs	Each partner will protect the data's confidentiality, through access regulation, VPN, Back-UPs	
Dissemination level (sensitive - SEN, public - PU)	SEN	SEN	SEN	SEN	SEN	
Deliverable	D4.1	D4.2	D4.3	D4.4	D4.5	
Classified information* (1 – yes, 0 – no)***					0	

Items	**WP5**		

	Task 5.1	***Task 5.2***	***Task 5.3***	***Task 5.4***	**Comments and potential risks of data management**
Name of dataset	Report on digital solutions deployment and demonstration in whitegoods sector- washing machine	Report on digital solutions deployment and demonstration in whitegoods sector-refrigerator	Report on digital solutions deployment and demonstration in electronics sector-printer	Report on digital solutions deployment and demonstration in automotive sector-automotive spare parts	
Type of data*	text	text	text	text	
Description of data					
Source/origin of data	Demo/users	Demo/users	Demo/users		
Format of data**	PDF, doc/docx, jpg, png	PDF, doc/docx, jpg, png	PDF, doc/docx, jpg, png	PDF, doc/docx, jpg, png	
Personal data (1 – yes, 0 – no)	0	0	0	0	
Responsible data controller	GORENJE	Arcelik	Lexmark	C-ECO	
Confidential information** (1 – yes, 0 – no)***	1	1	1	1	
Method(s) of access restriction to confidential information by partner	Each partner will protect the data's confidentiality.	Each partner will protect the data's confidentiality.	Each partner will protect the data's confidentiality.	Each partner will protect the data's confidentiality.	
Dissemination level (sensitive - SEN, public - PU)	PU	PU	PU	PU	
Deliverable	D5.1	D5.2	D5.3	D5.4	
Classified information*** (1 – yes, 0 – no)***					

Items	**WP6**				**Comments and potential risks of data management**
	Task 6.1	***Task 6.2***	***Task 6.3***	**Task 6.4**	
Name of dataset	Report on definition of KPIs	Report on evaluation of the demonstrators	Report on upscaling and business potential evaluation	Evaluation report of the upscaling potential at sector level	

Funded by the European Union

Type of data*	text	text	text	text	
Description of data					
Source/origin of data	Literature review and interviews with demos and technology providers	Demos/users	Demos/users		
Format of data**					
Personal data (1 – yes, 0 – no)					
Responsible data controller					
Confidential information*** (1 – yes, 0 – no)***					
Method(s) of access restriction to confidential information by partner					
Dissemination level (sensitive - SEN, public - PU)	PU	PU	SEN	SEN	
Deliverable	D6.1	D6.2	D6.3	D6.4	
Classified information**** (1 – yes, 0 – no)***					

Items	**WP7**			**Comments and potential risks of data management**
	Task 7.1	***Task 7.2***	***Task 27.3***	
Name of dataset	Demonstrator's synergy report	Training materials	Report on training execution and long-term training strategy	
Type of data*	text	Text	text	
Description of data				
Source/origin of data				
Format of data**				
Personal data (1 – yes, 0 – no)				
Responsible data controller				
Confidential information*** (1 – yes, 0 – no)***				
Method(s) of access restriction to				

confidential information by partner				
Dissemination level (sensitive - SEN, public - PU)	PU	SEN	SEN	
Deliverable	D7.1	D7.2	D7.3	
Classified information* (1 – yes, 0 – no)***				

Items	**WP8**									**Comments and potential risks of data management**
	Task 8.1	***Task 8.2***	***Task 8.3***	***Task 8.4***	***Task 8.5***	**Task 8.6**	**Task 8.7**	***Task 8.8***	***Task 8.9***	
Name of dataset	Standardisation report	Dissemination and communication plan and periodic D&C progress reports	Final report on the Dissemination and Communication Activities	Visual identity and website	Digital Helix ecosystem development and clustering reports	IPR registry	Exploitation strategy and plan report	Exploitation strategy and plan report UPDATE	Final report on synergies and collaboration	
Type of data*	text	text	text	Text, pictures	text	text	text			
Description of data										
Source/origin of data		Consortium partners	Consortium partners							
Format of data**										
Personal data (1 – yes, 0 – no)										
Responsible data controller										
Confidential information *** (1 – yes, 0 – no)		0	0	0	0	0	0	0	0	
Method(s) of access restriction to confidential information by partner										

Funded by the European Union

Dissemination level (sensitive – SEN, public - PU)	SEN	PU	PU	PU	PU	SEN	SEN	SEN	PU	
Deliverable	D8.1	D8.2	D8.3	D8.4	D8.5	D8.6	D8.7			
Classified information * (1 – yes, 0 – no)***		0	0	0	0				0	

Items	**WP9**			**Comments and potential risks of data management**
	Task 9.1	***Task 9.2***	***Task 9.3***	
Name of dataset	Project quality handbook	Initial data management plan	Final data management plan	
Type of data*	text	text	text	
Description of data				
Source/origin of data	Grant agreement, Consortium agreement	Demos/users	Demos/users	
Format of data**	.doc, pdf	.doc, pdf	.doc, pdf	
Personal data (1 – yes, 0 – no)	0	0	0	
Responsible data controller	Alena Klapalová, Farazee Asif Lucie Winklerová	Alena Klapalová, Farazee Asif Lucie Winklerová	Alena Klapalová, Farazee Asif Lucie Winklerová	
Confidential information (1 – yes, 0 – no)***	1	0	0	
Method(s) of access restriction to confidential information by partner	Tagged as sensitive; announcement to the granting authority	Not needed	Not needed	
Dissemination level (sensitive - SEN, public - PU)	SEN	PU	PU	
Deliverable	D9.1	D9.2	D9.3	
Classified information* (1 – yes, 0 – no)***				

12. Annex 2 Readme template[3]

Data Set Title: "[insert title as defined in the DMP]"

Data Set Author/s: Name Surname (Affiliation), ORCID (if available);

Data Set Contributor/s: Name Surname (Affiliation), ORCID (if available);

Data Set Contact Person/s: Name Surname (Affiliation), ORCID (if available), email;

Data Set License: this data set is distributed under a [insert LICENSE]

Publication Year: [insert YEAR]

Project Info: [DiCiM] ([Digital Value Management for Unlocking the potential of the Circular Manufacturing Systems with integrated digital solutions], funded by European Union, Horizon Europe Programme. Grant Agreement No. [101091536]; [dicimproject.eu]

Data set Contents

The data set consists of:

- • 1 tabular quantitative file saved in .csv format: "title"
- • 1 README file: "title"

Data set Documentation

Abstract:

[Insert data set abstract]

Content of the files:

- • file [Insert filename] contains ...
- • file [Insert filename] contains ...
- • ...

Notes

[Related to the whole dataset]

Data sources

[Optional]

Methodologies

[If necessary to understand how to reuse data]

Codebook of variables

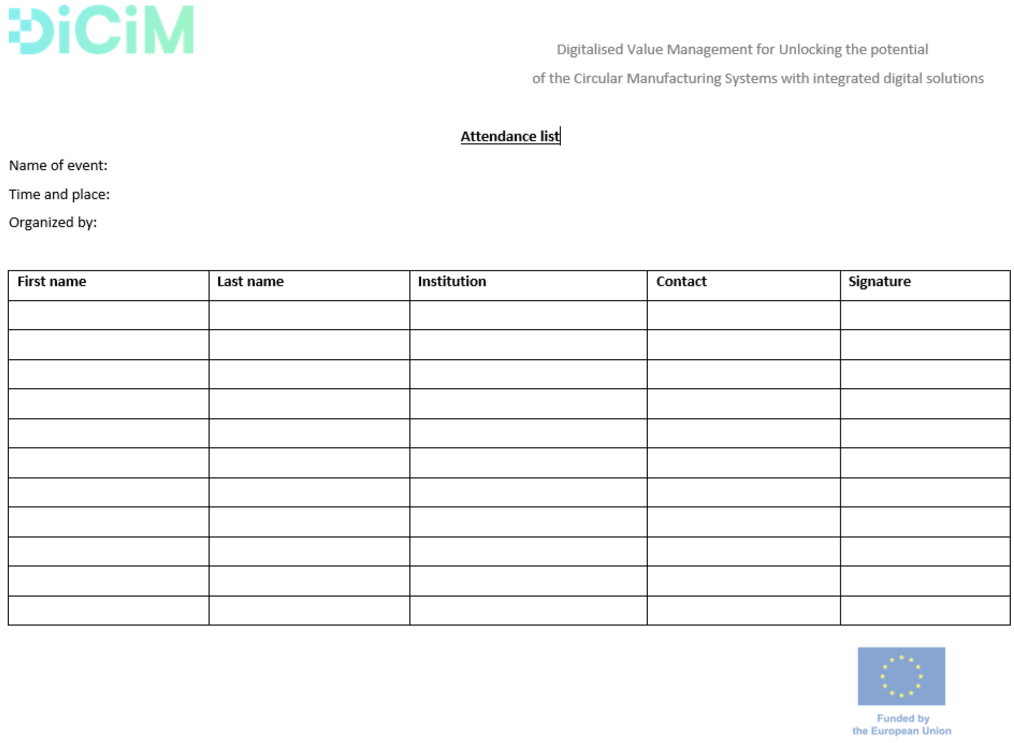
[If necessary to understand the meaning of the variables]

[3] This template was designed for the DMP of the project ABSTRACTION: UNLOCKING MEANING FROM EXPERIENCE THROUGH LANGUAGE, 2022 and only slightly adapted. Full authorship is hold by Marianna Bolognesi . DMP is available here: http://amsacta.unibo.it/id/eprint/7110/

Funded by the European Union

13. Annex 3 Attendance list template

preview of the document form available in MS Teams



Digitalised Value Management for Unlocking the potential
of the Circular Manufacturing Systems with integrated digital solutions

Attendance list

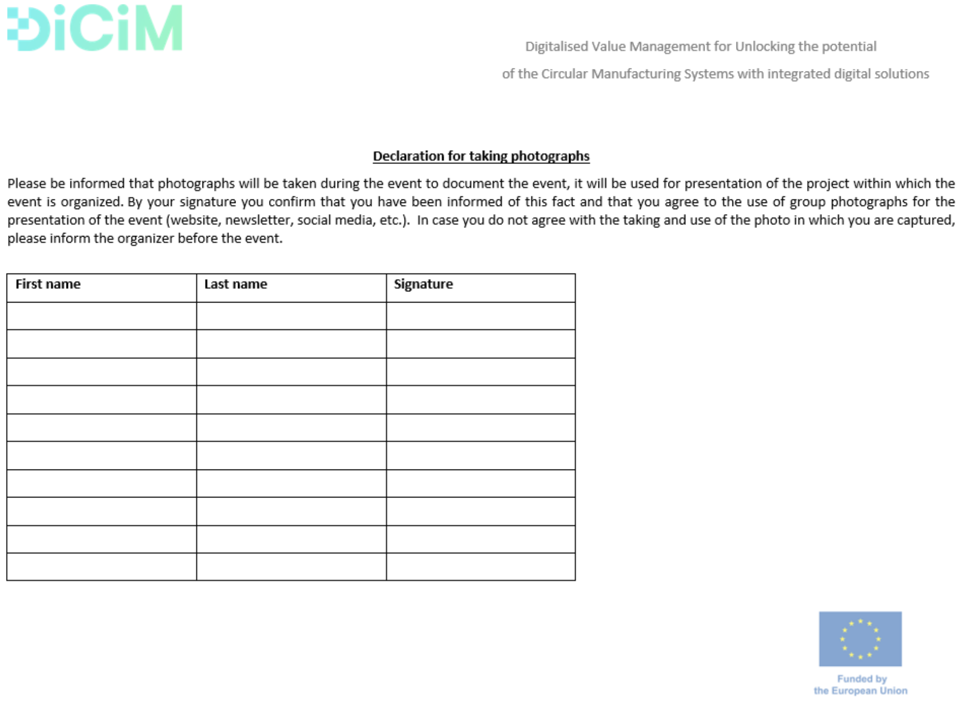
Name of event:

Time and place:

Organized by:

First name	Last name	Institution	Contact	Signature

Funded by
the European Union



Digitalised Value Management for Unlocking the potential
of the Circular Manufacturing Systems with integrated digital solutions

Declaration for taking photographs

Please be informed that photographs will be taken during the event to document the event, it will be used for presentation of the project within which the event is organized. By your signature you confirm that you have been informed of this fact and that you agree to the use of group photographs for the presentation of the event (website, newsletter, social media, etc.). In case you do not agree with the taking and use of the photo in which you are captured, please inform the organizer before the event.

First name	Last name	Signature

Funded by
the European Union

Funded by
the European Union

Attendance list

Name of event:

Time and place:

Organized by:

First name	Last name	Institution	Contact	Signature

Funded by
the European Union

<u>Declaration for taking photographs</u>

Please be informed that photographs will be taken during the event to document the event, it will be used for presentation of the project within which the event is organized. By your signature you confirm that you have been informed of this fact and that you agree to the use of group photographs for the presentation of the event (website, newsletter, social media, etc.). In case you do not agree with the taking and use of the photo in which you are captured, please inform the organizer before the event.

First name	**Last name**	**Signature**

Funded by
the European Union