Co-funded by the European Union

CYCERONE Cybersecurity academy for education and experience

Deliverable D1.2: Data Management Plan

Deliverable D1.2

Contractual Date:	**31-03-2025**
Actual Date:	**19-03-2025**
Grant Agreement No.:	**101189986**
Work Package:	**WP1**
Task Item:	**T1.2**
Lead Partner:	**EITD**
Authors:	Vilma Djala, Luisa Focacci (EITD)

Abstract

This Data Management Plan (DMP) outlines how data within the project is managed in a FAIR (findable, accessible, interoperable, and reusable) manner. The DMP has been created in accordance with the Horizon Europe Data Management Plan Template. The DMP should include information on handling research data during and after the end of the project, what data will be collected, processed, and/or generated, how data will be curated and preserved, and other relevant issues. By following the guidelines outlined in the DMP, project partners follow the DMP and ensure that data is managed to maximise its value and impact.

The activities leading to these results has received funding from the European Community's DIGITAL Programme under Grant Agreement No. 101189986 (CYCERONE).

Versioning and contribution history

Version	Date	Author/s	Notes
0.1	05/02/2025	Vilma Djala (EITD)	First version of D1.1
0.2	20/02/2025	Asja Kamenica (EITD)	First review of D1.2
0.3	14/03/2025	Luisa Focacci, Vilma Djala (EITD)	Second version of D1.2
0.4	28/03/2024	Luisa Focacci (EITD)	Third Review of D1.2, Update of formats, fonts, insertion of approved logo

The activities leading to these results has received funding from the European Community's DIGITAL Programme under Grant Agreement No. 101189986 (CYCERONE).

List of Contents

List of Tables

1. Introduction

This Data Management Plan has been created following the Horizon 2020 FAIR DMP template, designed to apply any Horizon 2020 project that produces, collects or processes research data.

This document is intended to follow the best practices for a FAIR data management[1].

Definition: FAIR data management

In general terms, your research data should be "FAIR", that is findable, accessible, interoperable and re-usable. These principles precede implementation choices and do not necessarily suggest any specific technology, standard, or implementation-solution.

This Data Management Plan is a set of questions, from the Horizon 2020 template that were answered with a level of detail appropriate to the project. This DMP is intended to be a living document in which information can be made available on a finer level of granularity through updates as the implementation of the project progresses and when significant changes occur.

Scope is the consistently proper treatment of all data generated and/or to be maintained within CYCERONE Project media. The underlying objective is the handling and management of all data with the utmost care for security, compliance, and long-term utility, pointing to the methodology used, within the broad General Data Protection Regulation (GDPR) framework. The DMP outlines a comprehensive data collection, storage, and preservation framework, adhering to the highest standards to maintain data integrity and accessibility.

As a minimum, the DMP should be updated in the context of the periodic evaluation/assessment of the project. If there are no other periodic reviews envisaged within the grant agreement, an update needs to be made in time for the final review at the latest.

1.1 CYCERONE

CYbersecurity aCadEmy foR educatiOn and experieNcE (CYCERONE) aims at:

- Offering a unified access point for diverse learners – focusing on SMEs and public sectors - to enhance their cybersecurity skills,
- Amplifying the reach of higher education institutions and professional training providers in cybersecurity through strategic marketing and dissemination within the Cybersecurity Skills Academy, connecting to existing available tools, such as the EU Digital Skills and Jobs Platform and ENISA's CyberHEAD Database,

---

[1] FAIR Data Principles (FORCE11 discussion forum): https://force11.org/group/fairgroup/fairprinciples

FAIR principles (article in Nature): https://www.nature.com/articles/sdata201618

- Mitigating the cybersecurity talent gap in Europe by making skilled professionals more accessible across various industry sectors.

2. Work Package 1

The objectives of Work Package 1 are as follows:

- Oversee project management and provide effective administrative, technical, and financial support ensuring high-quality content and management best practices that drive meaningful project progress.
- Coordinate the participant enrolment process for the CYCERONE learning programs.
- To foster the creation of effective and sustainable partnerships within the project consortium.

This work package focuses on leading the technical and scientific coordination of the CYCERONE project, along with its administrative and financial management. It will also implement quality control and reporting mechanisms throughout the project.

3. Deliverable 1.2

3.1 Purpose

The CYCERONE Data Management Plan has been prepared with two purposes:

1. To describe the data management life cycle for the data to be collected, generated, and processed by the CYCERONE project;
2. To include information on the handling of research data during and after the end of the project, what data will be collected, processed and/or generated, how data will be preserved, and resource and budgetary planning for data management.

3.2 Objectives

- Ensure effective management of research data throughout the project life cycle.
- Describe the data management life cycle for the data to be collected, processed and/or generated by the project.
- Ensure that research data is findable, accessible, interoperable and re-usable (FAIR).
- Ensure that research data is managed in compliance with the General Data Protection Regulation (GDPR).
- Reflect the current state of consortium agreements on data management and be consistent with Exploitation and Intellectual Property Rights (IPR) requirements.
- Provide an overview of all datasets collected and generated by the project and define the consortium's data management policy and approach.

4. Data summary

This is an overview of the different data sets that are currently, and will be, produced in the CYCERONE project. We need to distinguish between two types of data:

1. Non-sensitive data produced by the project, publicly available and released for potential reuse in other projects or research activities.
2. Operational data used to implement the activities described in the project. This data includes potentially sensitive data about students and participants in training activities if and in which forms, if any, is shared, unsolicited, by students via their CVs or communications of interest in participating in the CYCERONE-scoped activities.

The following table shows the data type, the origin of the data, the related WP number and the format in which the data will be expected to be stored.

Table 1: Data sets overview

#	*Data type*	*Type*	*Origin*	*WP#*	*Format*
1	Market review of labour needs in Cybersecurity	Non-sensitive	Data was derived from the reports and market data.	WP1, WP2	.pdf
2	Literature review data on Cybersecurity	Non-sensitive	Derived data, coming from publications or published reports.	WP1, WP2	.pdf
3	Recruitment cycle data about participants.	Operational	Primary data	WP1, WP2	.xlsx and .docx and .pdf
4	Personal data of students participating in learning programmes.	Non-sensitive	Primary data	WP1, WP2	.xlsx and .pdf and university systems
6	Satisfaction survey from students at the end of a learning course or activity.	Operational except for personal student information if any arising from CV. None expected at this time.	Primary data	WP3, WP4	.xlsx and .pdf
7	Marketing data related to communication and dissemination activities.	Operational	Primary data	WP2	.xlsx and .pdf

Table 2 describes the data set and the purpose of the collection of generated data in relationship with the objectives of the project. Additionally, it shows the data utility by clarifying to whom the data might be useful.

Table 2: Data sets description and utility

#	Data type	Description & Purpose	Utility
1	Labour Market needs review	**Description** The data contains the result of a market review analysis done in the field of Cybersecurity. The study will be performed by analysing publicly available market data and interviewing economic actors in the sector.	The data could be useful for research on the Cybersecurity sectors. It can also be useful for other educational institutions and to organisations and businesses to better understand the current state of the market, identify the latest trends and threats and

#	Data type	Description & Purpose	Utility
		Purpose The collection of this data will serve the course-review process and training programmes review. This data will also serve as guide to the definition of the content for the self-standing learning modules.	make informed decisions about Cybersecurity products and services.
2	Literature review data on Cybersecurity.	**Description** The data contains the result of a literature review done in the field of cybersecurity. The analysis will be performed by analysing publications, articles and course syllabi from other universities and higher education institutions. **Purpose** The collection of this data will serve as input to the process of reviewing of the courses and training programmes provided under the CYCERONE platform. This data will also serve to guide the definition of the learning content.	The data could be helpful to researchers interested in understanding the current state of knowledge in the field of Cybersecurity, identifying gaps in the literature and developing research questions and hypotheses. The data can also be useful for policymakers by helping develop evidence-based and effective policies and regulations.
3	Recruitment cycle data about participants.	**Description** This data includes all the personal information of candidates applying for learning programmes. The data will consist of contact information, CV history and study track records for all applicants. **Purpose** Data is gathered for administrative purposes and to enable the selection of candidates.	Researchers can use this data, after anonymisation, to study the qualifications and backgrounds of candidates applying for programmes or jobs. The data can help researchers identify trends and patterns in the qualifications and backgrounds of successful candidates and develop research questions and hypotheses. Personal data could be shared with relevant third parties (i.e. employers or recruitment agencies) upon collecting individual and informed consent of participants.
4	Personal data of students participating in learning programmes.	**Description** This data includes all the personal information of participants in our courses and programmes. The data will include contact information, CV history and study track records for all students and will be managed by the guesting universities following the general rules for all students. **Purpose** Data is gathered for administrative purposes (i.e. admission process) to enable participation in the courses and track the student's academic pathway.	Researchers can use this data, after anonymisation, to study the qualifications and backgrounds of learners of the self-standing modules. The data can help researchers identify trends and patterns in the qualifications and backgrounds of online students and develop research questions and hypotheses. Personal data could be shared with relevant third parties (i.e. employers or recruitment agencies) upon collecting individual and informed consent of students.

#	Data type	Description & Purpose	Utility
5	Satisfaction survey from students at the end of a learning course or activity.	**Description** Data related to the results of the satisfaction survey gathered from participants to our programmes. **Purpose** Data is gathered to implement a quality improvement process and to improve courses and training material.	The data is of interest to the project participants to obtain workable feedback and encourage a continuous improvement cycle of the course's materials and training paths. It will not be publicly available unless anonymised.
6	Marketing data related to communication and dissemination activities.	**Description** Data regarding the communication and dissemination campaign on social networks and digital channels. **Purpose** Digital marketing will be a central part of the strategy to attract candidate students to the project's programmes. Collecting operational data is fundamental for digital communication to work effectively.	The anonymised data could be helpful to digital marketing agencies or marketing professionals interested in evaluating the effectiveness of their digital marketing campaigns and identifying areas for improvement. Researchers can use this anonymised data to study the effectiveness of digital marketing campaigns and identify trends and patterns in the participation of potential students or customers.

5. FAIR Data

5.1 Making data findable, including provisions for metadata

To ensure that the data generated during the project is clear and easy to find, we will implement the following provisions:

- All data will be recorded in a predeterminate structure and with agreed data formats.
- Data structure and format will ensure interoperability and ease of use.
- To ensure that the data is discoverable, we will implement the following mechanisms:
  - Data will be assigned unique identifiers to enable straightforward identification and fast tracking.
  - Data will be stored in a structured and organised manner to enable efficient searching and browsing.
  - Data will be made available through appropriate repositories and archives to enable discovery and reuse.

5.2 Making data accessible

The following table highlights which data is intended for internal use (within the CYCERONE project) and which will be made openly available. It also explains why several datasets cannot be shared for specific reasons, and, in this case, an alternate solution will be presented.

Table 3: Data sets accessibility

#	Data type	Openly available	Justification	Alternate solution
1	Labour Market needs review	Yes	Results of this analysis will be described in the project deliverable D4.2.	*(not relevant)*
2	Literature review data on cybersecurity	Yes	Results of this review will be described in the project deliverable D1.1.	*(not relevant)*
3	Recruitment cycle data about participants.	No	The sensitive data, if any, arising from recruitment will not be shared, according to GDPR data policy	*(not applicable)*
4	Data of students participating in online training units, modules and courses	No	The sensitive data, if any about students participating in the project's courses and learning activities will not be released, according to GDPR and any other regulation that may apply.	Statistical data about the student participation in the portfolio of courses and programmes will be described in the project deliverables connected to WP3 and WP4.
5	Satisfaction survey from students at the end of a learning course or activity.	No	All participants' personal data, including contact information and opinion on the course quality, will not be made openly available, according to GDPR and any other regulation that may apply.	Statistical data about the student satisfaction expressed for the courses attended will be described in the project deliverables for WP4.
6	Marketing data related to communication and dissemination activities.	No	The granular and analytical marketing data used to guide communication and dissemination activities will not be released.	Aggregated statistical data about marketing and dissemination activities will be released in deliverables D2.1, D2.2, D2.3, D2.4.

The data intended for open availability will be registered in official project deliverables and, as such, will be published on the project website and on the EC portal for public access.

5.3 Making data interoperable

All the data shared by and for the project will use document standards that will make it interoperable. The aim is to achieve a standardised, open, and flexible way to exchange and reuse data across different systems and applications.

5.4 Increase data re-use (through clarifying licences)

All openly available project deliverables and main results will be released with a Creative Commons Attribution (CC-BY) license to permit the widest re-use of data. This license allows others to distribute, remix, and build upon the data, even commercially, as long as they credit the original source.

The data released under this license does not include:

- Any sensible information regarding students that will be protected by GDPR and other relevant regulations,
- The programmes and course materials that will remain the property of the producing entity, and
- The online training modules that will maintain shared ownership between the beneficiaries who have generated them.

6. Allocation of resources

The following resources will be allocated to ensure effective data management throughout the project:

- **Personnel**: Data management will be overseen in Task 1.2 of the WP1. The task will permit all partners involved in these activities to dedicate resources, including personnel, to the tasks and activities related to data management. A data manager will be appointed to oversee the implementation of the data management plan and ensure compliance with relevant regulations and guidelines. The data manager will be responsible for creating and maintaining the metadata, ensuring data quality, and managing the storage and security of the data. The data manager will also be accountable for training project personnel in data management best practices.
- **Infrastructure**: The project will allocate resources for the storage and backup of data in secure locations. For this purpose, the project will use the website and the Teams instance of the coordinator partner, EIT Digital.
- **Budget**: The project will allocate a budget for data management activities. The budget will also include provisions for disseminating and sharing data, including use of appropriate repositories and archives.
- **Deliverables**: This deliverable D1.2 of the project describes an initial data management plan. The project will also include deliverables for the dissemination and sharing of data in accordance with WP2 once deliverables are complete and available for the whole project members' audience.

The allocation of resources will be reviewed and updated throughout the project as necessary to ensure that the data management plan remains effective and compliant with relevant regulations and guidelines. The project will also ensure that the allocation of resources is consistent with Exploitation and Intellectual Property Rights (IPR) requirements.

7. Data Security

The project will implement the following measures to ensure the security of the data recorded on the Microsoft Teams platform used to store all relevant project data:

- **Access controls**: Access to the data will be restricted to authorised personnel only. The project will use Microsoft Teams to manage access controls, including role-based access controls and multi-factor authentication.
- **Backup and recovery**: The project will implement a backup and recovery plan to ensure that the data is recoverable in the event of a disaster or system failure. The project will use the Microsoft platform backup and recovery capabilities to ensure that the data is protected.

- **Data retention and disposal**: The project will implement a data retention and disposal policy to ensure that data is retained only for as long as necessary and disposed of securely when it is no longer needed.
- **Monitoring and auditing**: The project will implement monitoring and auditing procedures to ensure that the data is being used appropriately and that any unauthorised access or use is detected and addressed.

The project will also ensure that all personnel involved in the project are briefed in data security best practices and understand their roles and responsibilities in protecting the data. The project will also ensure that all data management activities comply with all relevant regulations and guidelines, to include those not referenced in this DMP.

8. Ethical Aspects

The project will ensure that all data management activities are conducted in compliance with relevant ethical guidelines and regulations. The following ethical aspects will be considered:

1. **Informed consent**: The project will obtain informed consent from all participants before collecting any data. Participants will be informed about the purpose of the data collection, how the data will be used, and any potential risks or benefits associated with the data collection.
2. **Data privacy**: The project will ensure that all data is collected, stored, and shared in compliance with relevant data privacy regulations. The project will implement appropriate measures to protect the privacy and confidentiality of the data, including encryption, access controls, and data anonymisation where necessary.
3. **Data ownership**: The project will ensure that all data is owned by the appropriate parties and that any intellectual property rights are respected. The project will also ensure that any data sharing or dissemination is conducted in compliance with relevant regulations and guidelines.
4. **Data sharing**: The project will ensure that any data sharing or dissemination is conducted in compliance with relevant regulations and guidelines. The project will also ensure that any data sharing or dissemination is conducted in a manner that respects the privacy and confidentiality of the data.
5. **Data retention and disposal**: The project will implement a data retention and disposal policy to ensure that data is retained only for as long as necessary and disposed of securely when it is no longer needed.

9. Other issues

Data management in the project will be performed following the European Commission's Horizon 2020 procedures. This document represents the Data Management Plan (DMP) as requested in the programme. It describes the data management life cycle for the data to be collected, processed, and/or generated by the project.

References

[DIGITAL] https://digital-strategy.ec.europa.eu/en/activities/digital-programme

[CYCERONE] https://eitictlabs.sharepoint.com/sites/Cycerone

Glossary

Community	A group of users organised with a common purpose and jointly granted access to resources. It may act as the interface between individual users and the resources. (see also [WISE-SCI])
EC	European Commission
EIT	European Institute of Innovation and Technology
KIC	Knowledge and Innovation Community
GA	Grant Agreement
GDPR	General Data Protection Regulation (see https://gdpr.eu/)