31-05-2025

Deliverable D4.2:

Data Management Plan

Deliverable D4.2

Contractual Date:	28-02-2024
Actual Date:	31-05-2025
Grant Agreement No.:	101123118
Work Package:	WP4
Task Item:	T4.2
Lead Partner:	EITD

Authors: Andrea Biancini (EITD), Romane Léauté (EITD)

Abstract

Central to the project is the Data Management Plan (DMP), which ensures that all data generated and handled is managed with the utmost care for security, compliance, and long-term utility. The DMP outlines a comprehensive framework for data collection, storage, and preservation, adhering to the highest standards to maintain data integrity and accessibility. By establishing clear roles and responsibilities among project partners and implementing rigorous data security measures, the DMP safeguards sensitive information while promoting transparency and effective collaboration.

The activities leading to these results has received funding from the European Community's DIGITAL Programme under Grant Agreement No. 101123118 (SPECTRO).

Versioning and contribution history

Version	Date	Authors	Notes
0.1	07/11/2023	Andrea Biancini (EITD)	Draft version.
0.2	30/11/2023	Andrea Biancini (EITD)	Accepted revisions from partners.
0.3	05/02/2024	Andrea Biancini (EITD)	Integrated information form UNITN regarding data formats, long term preservation and other modifications.
0.4	11/04/2025	Romane Léauté (EITD)	Restructured deliverable according to PO comments during review meeting.
0.5	31/05/2025	Romane Léauté (EITD)	Restructured deliverable according to PMON comments after the review meeting.

Table of Contents

Table of Figures

No table of figures entries found.

Table of Tables

1 Introduction

The Data Management Plan (DMP) is a critical deliverable within the SPECTRO project, guiding the management of data throughout the project's lifecycle. It outlines the principles and procedures that will be applied to ensure that all data generated, collected, processed, and shared within the project is handled in a manner that supports the integrity, security, and availability of information. In accordance with the Digital Europe Programmes' (DEP) data management guidelines, this DMP is structured to align with the FAIR (Findable, Accessible, Interoperable, Reusable) principles, ensuring that data remains an accessible and reusable asset for stakeholders both within and beyond the project's duration. 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.

The SPECTRO project, which focuses on specialised education in Cybersecurity and Robotics, generates a diverse array of data—including technical documentation, educational content, participant records, and stakeholder feedback. Effective data management is therefore essential to ensure that this information is handled optimally, supporting both the project's educational and research objectives while maintaining the highest standards of security and confidentiality where required.

This Data Management Plan (DMP) defines the protocols for the collection, processing, storage, sharing, and long-term preservation of data within SPECTRO. It ensures that all partners are aligned in their approach to data management, mitigating risks related to data loss, breaches, or misuse. The DMP also provides a framework to ensure compliance with European Union regulations on data protection, privacy, and security—including the General Data Protection Regulation (GDPR).

A key objective of the SPECTRO DMP is to balance the need for data accessibility—to facilitate research, educational improvements —with the obligation to protect sensitive and personal information, particularly that of students and programme participants. The plan supports transparent and structured data handling, fostering collaboration among project partners from multiple countries and sectors, each with their own data management requirements and practices.

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

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

The DMP covers all data types managed throughout the project lifecycle, including research data, operational data, personal data, and metadata. It outlines the roles and responsibilities of partners in managing data, ensuring compliance with the plan, and detailing measures for safeguarding data integrity and confidentiality.

Ultimately, the aim is to ensure that data produced by SPECTRO becomes a valuable resource for future research, educational innovation, and policy development. By adhering to FAIR (Findable, Accessible, Interoperable, Re-usable) principles and best practices in data management, and ensuring compliance with ethical, legal, and security standards, the DMP will maximize the long-term impact of the project's outputs and contribute to advancing digital skills and knowledge in Europe

1.1 SPECTRO

SPecialised Education programmes in CybersecuriTy and Robotics (SPECTRO) will focus on the design and delivery of two double-degree master's programmes (ISCED Level 7, 120 ECTS) in two key digital technology areas for the future of Europe: (1) Cybersecurity, and (2) Robotics. The two specialised master's programmes, which will also include a minor in Innovation and Entrepreneurship, will be designed and delivered by a consortium consisting of 14 higher education institutions (7 of which involved in Cybersecurity and 10 in Robotics) from 8 different countries , 2 innovative SMEs, 1 leading research centre in Information Systems and EIT Digital, a pan-European organisation with in-depth knowledge and experience in the digital skills domain.

The master's programmes developed by SPECTRO partners will address the labour market needs, foster strong interactions and mobility between academia and business, strengthen knowledge triangle integration, promote entrepreneurship, and considerably boost the growth of the existing EIT Digital ecosystem, one of the largest digital ecosystems in Europe. In addition to the two master's programme, SPECTRO partners will also develop and deploy a series of self-standing learning modules on topics related to Cybersecurity and Robotics. These modules will lead to four different certifications, which will be released by participating higher education institutions and EIT Digital. Dedicated marketing, promotion, communication, and dissemination activities will be carried out by SPECTRO partners to maximise the outreach of project activities and to attract the desired target audience to the master's programmes and self-standing modules. SPECTRO will expand the specialised education offer in Europe and will contribute to reducing the current shortage of digital specialists in Europe, by providing training to more than 1000 European citizens in Cybersecurity and Robotics.

1.2 Work Package 4

The objectives of Work Package 4 are:

- To ensure the overall management of the project and effectively monitor the project, in administrative, technical, and financial terms.
- To guarantee high-quality content and management with the aim of securing effective progress.
- To coordinate the enrolment process of participants to SPECTRO education programmes.
- To ensure the establishment of effective and sustainable partnerships within the consortium.

It is concerned with undertaking the technical and scientific coordination of the SPECTRO project as well as the administrative and financial management. This work package will ensure that appropriate quality control and reporting mechanism are applied across the project.

1.3 Deliverable 4.2

1.3.1 Purpose

The SPECTRO Data Management Plan has been prepared with these two purposes:

1. to describe the data management life cycle for the data to be collected, processed and/or generated by the SPECTRO project;
2. 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 curated and preserved, and resource and budgetary planning for data management.

1.3.2 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.

2 Data Summary

2.1 Data sets overview and description

In order to provide an overview of the different data sets that are currently and will be produced in the SPECTRO project, we need to distinguish two types of data:

1. Non-sensitive data produced by the project 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 very frequently also sensitive data about students and participants to training 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 presumably stored.

#	Data type	Type	Origin	WP#	Format
1	Market review of Cybersecurity sector.	Non-sensitive	Derived data by other reports and market data.	WP1	PDF
2	Market review of Robotics sector.	Non-sensitive	Derived data by other reports and market data.	WP2	PDF
3	Literature review data on Cybersecurity.	Non-sensitive	Derived data by publications or published reports.	WP1	PDF
4	Literature review data on Robotics.	Non-sensitive	Derived data by publications or published reports.	WP2	PDF
5	Recruitment cycle data about participants (incl. FSTP applicants)	Operational	Primary data	WP1, WP2	CSV and PDF
6	Personal data of students participating to master programmes.	Operational	Primary data	WP1, WP2	CSV
7	Data on participants to self-standing modules.	Operational	Primary data	WP1, WP2	CSV
8	Satisfaction survey from students at the end of a learning course or activity.	Operational	Primary data	WP1, WP2	CSV
9	Marketing data related to communication and dissemination activities.	Operational	Primary data	WP3	CSV

Table 1: Data sets overview

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

#	Data type	Description & Purpose	Utility
1	Market review of Cybersecurity sector.	**Description** The data contains the result of a market review analysis done on the field of cybersecurity. The analysis will be performed by analyzing publicly available market data and by interviewing economic actors in the sector. **Purpose** The collection of this data will serve as an input to the process of review of the master program curriculum. This data will also serve to guide the definition of the content for the self-standing learning modules.	The data could be useful for research on the cybersecurity sector. It can also be useful for other educational institutions and to organizations and business to better understand the current state of the market, identify the latest trends and threats and make informed decisions about cybersecurity products and services.

#	*Data type*	*Description & Purpose*	*Utility*
2	Market review of Robotics sector.	**Description** The data contains the result of a market review analysis done on the field of robotics and autonomous systems. The analysis will be performed by analyzing publicly available market data and by interviewing economic actors in the sector. **Purpose** The collection of this data will serve as an input to the process of review of the master program curriculum. This data will also serve to guide the definition of the content for the self-standing learning modules.	The data could be useful for research on the robotics and autonomous systems sector. It can also be useful for other educational institutions and to organizations and business to better understand the current state of the market, identify the latest trends and threats and make informed decisions about robotics products and services.
3	Literature review data on Cybersecurity.	**Description** The data contains the result of a literature review done on the field of cybersecurity. The analysis will be performed by analyzing publications, articles and course syllabus from other universities and higher education institutions. **Purpose** The collection of this data will serve as an input to the process of review of the master program curriculum on cybersecurity. This data will also serve to guide the definition of the content for the self-standing learning modules.	The data could be helpful to researcher interested in understanding the current state of knowledge in the field of cybersecurity, identify gaps in the literature and develop research question and hypotheses. The data can also be useful for policymakers by helping the development of policies and regulations that are evidence-based and effective.
4	Literature review data on Robotics.	**Description** The data contains the result of a literature review done on the field of cybersecurity. The analysis will be performed by analyzing publications, articles and course syllabus from other universities and higher education institutions. **Purpose** The collection of this data will serve as an input to the process of review of the master program curriculum on cybersecurity. This data will also serve to guide the definition of the content for the self-standing learning modules.	The data could be helpful to researcher interested in understanding the current state of knowledge in the field of cybersecurity, identify gaps in the literature and develop research question and hypotheses. The data can also be useful for policymakers by helping the development of policies and regulations that are evidence-based and effective.

#	*Data type*	*Description & Purpose*	*Utility*
5	Recruitment cycle data about participants (incl. FSTP applicants)	**Description** This data includes all the personal information of candidates applying for the master programmes. The data will include 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, including the awarding of scholarships, based on their recent educational and professional history.	Researchers can use this data, after anonymization, to study the qualifications and backgrounds of candidates applying for master's 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 collection of individual and informed consent of participants.
6	Personal data of students participating to master programmes.	**Description** This data includes all the personal information of students of the master 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 and to enable participation to the courses and track of the student's path.	Researchers can use this data, after anonymization, 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 collection of individual and informed consent of students.
7	Data on participants to self-standing modules.	**Description** Data related to the registration and participation to self-standing modules. This data includes contact information and digital addresses of all participants. The data also includes information regarding eventual certifications obtained by the participants. **Purpose** Data is gathered for administrative purposes to enable the access to the online platform and the tracking of the study activities.	Researchers can use this data, after anonymization, 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 collection of individual and informed consent of participants.
8	Satisfaction survey from students at the	**Description** Data related to the results of the satisfaction survey gathered from students of master and self-standing modules.	The data is of interest to the project participants to obtain workable feedback and encourage continuous improvement cycle of the courses materials and trainings

#	*Data type*	*Description & Purpose*	*Utility*
	end of a learning course or activity.	**Purpose** Data is gathered to implement a quality improvement process and to improve courses and training material.	paths. It will not be publicly available unless anonymized.
9	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 of attraction to candidate students to the project's program. Collecting operational data is fundamental for digital communication to work effectively.	The anonymized data could be helpful to digital marketing agencies or marketing professional interested in evaluating the effectiveness of their digital marketing campaigns and identify areas for improvement. Researchers can use this anonymized data to study the effectiveness of digital marketing campaigns and identify trends and patterns in the participation of potential students or customers.

Table 2: Data sets description and utility

Table 3: Data processing operations is a structured overview of the main data processing operations identified, the types of data collected for each, the responsible partner, and the relevant privacy or data protection statements where applicable.

#	Operation	Data Collected	Privacy Statement	*Responsible partner*
1	Surfing the Websites	IP address, browser type, device information, usage statistics, cookies	For SPECTRO webpages: EIT Digital Privacy policy	For SPECTRO webpages: EIT Digital Each partner is responsible for their own website data collection and processing
2	Enrolling in Master's Programme	Name, contact details, educational background, nationality, application documents, consent status	EIT Digital Privacy policy, Master School Terms and Conditions, Student Agreement Contract	EIT Digital
3	Enrolling in online self-standing modules	Name, contact details, educational background, nationality, consent status	EIT Digital Privacy policy and Icarus AI Privacy Policy	Eit Digital and Evolutionary Archetypes

#	Operation	Data Collected	Privacy Statement	*Responsible partner*
4	Participating in Surveys	Responses to survey questions, possibly demographic data, consent status	Data anonymized or pseudonymized where possible; used for project evaluation and reporting.	Each partner is responsible for their own survey data collection and processing
6	Registering for Events	Name, contact details, event preferences, consent status	Data used for event organization and follow-up; retained as required for project reporting.	Each partner is responsible for their own event data collection and processing
7	Applying for Scholarships/FSTP Funding	Name, contact details, academic records, financial information, eligibility documents, consent status	EIT Digital Privacy policy, Master School Terms and Conditions, Student Agreement Contract	EIT Digital

Table 3: Data processing operations

2.2 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:

1. **Access controls**: Access to the data will be restricted to authorized personnel only. The project will use Microsoft Teams to manage access controls, including role-based access controls and multi-factor authentication.
2. **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's platform backup and recovery capabilities to ensure that the data is protected.
3. **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.
4. **Monitoring and auditing**: The project will implement monitoring and auditing procedures to ensure that the data is being used appropriately and that any unauthorized access or use is detected and addressed.

The project will also ensure that all personnel involved in the project are trained in data security best practices and that they understand their roles and responsibilities in protecting the data. The project will also ensure that all data management activities are compliant with relevant regulations and guidelines.

2.3 Data breach mitigation and corrective measures

In case of a data breach, here are general recommended key steps to take after detecting the breach:

1. **Contain the Breach**

The first critical action is to contain the breach and prevent further unauthorized access. This involves:

- Isolating compromised systems from the network
- Revoking access for potentially compromised users
- Securing affected systems to stop ongoing data leakage

2. **Activate Response Team**

Quickly assemble and activate an incident response team, including IT security specialists, legal representatives, and communications professionals. Brief key executives and establish a centralized communication channel.

3. **Assess the Situation**

Conduct a rapid assessment to determine:

- What data was exposed and who it belongs to
- The scope and impact of the breach
- Which systems were affected
- Potential vulnerabilities that led to the breach

4. **Document Everything**

Create a detailed timeline of the breach discovery, all response actions taken, and decisions made. This documentation is crucial for investigations, and regulatory reporting.

5. **Notify Relevant Parties**

Determine who needs to be notified based on legal requirements and the nature of the compromised data. This may include:

- Affected individuals
- Law enforcement
- Regulatory bodies
- Business partners

6. **Secure Systems and Data**

Take immediate steps to enhance security:

- Change access credentials for all affected accounts

- Enable additional security measures like encryption
- Restrict access to sensitive data and systems

7. **Initiate Investigation**

Work with relevant experts to:

- Analyze logs and system access
- Determine the root cause of the breach
- Identify and implement necessary remedial measures

The Data Protection Officer (DPO) of the project can be reached at the following address, for any question or requests: privacy@eitdigital.eu

The table below presents, for each data type, the breach occurrence likelihood, preventive mitigation measures and recommended corrective measures in case of a breach.

#	***Data type***	***Breach Occurrence Likelihood***	***Mitigation measures (preventive)***	***Recommended corrective measures***
1	Market review of Cybersecurity sector.	Low	- Implement secure storage and access control to authorized personnel only. - Use private communication channels for sharing with restricted access to authorized personnel only.	- Notify researchers and collaborators. - Contain the breach by revoking unauthorized access. - Conduct a root cause analysis. - Strengthen data-sharing protocols.
2	Market review of Robotics sector.	Low	- Implement secure storage and access control to authorized personnel only. - Use private communication channels for sharing with restricted access to authorized personnel only.	- Notify researchers and collaborators. - Contain the breach by revoking unauthorized access. - Conduct a root cause analysis. - Strengthen data-sharing protocols.
3	Literature review data on Cybersecurity.	Low	- Implement secure storage and access control to authorized personnel only. - Use private communication channels for sharing with restricted access to authorized personnel only.	- Notify researchers and collaborators. - Contain the breach by revoking unauthorized access. - Conduct a root cause analysis. - Strengthen data-sharing protocols.

#	*Data type*	*Breach Occurrence Likelihood*	*Mitigation measures (preventive)*	*Recommended corrective measures*
4	Literature review data on Robotics.	Low	- Implement secure storage and access control to authorized personnel only. - Use private communication channels for sharing with restricted access to authorized personnel only.	- Notify researchers and collaborators. - Contain the breach by revoking unauthorized access. - Conduct a root cause analysis. - Strengthen data-sharing protocols.
5	Recruitment cycle data about participants (incl. FSTP applicants)	Medium	- Implement secure storage and access control to authorized personnel only. - Anonymize sensitive information, when possible	- Notify affected participants about the breach. - Provide guidance on monitoring for identity theft. - Implement stricter access control mechanisms.
6	Personal data of students participating to master programmes.	Low	- Implement secure storage and access control to authorized personnel only. - Anonymize sensitive information, when possible	- Report the breach to relevant authorities - Inform students promptly and offer support services - Provide guidance on monitoring for identity theft. - Implement stricter access control mechanisms.
7	Data on participants to self-standing modules.	Low	- Implement secure storage and access control to authorized personnel only. - Anonymize sensitive information, when possible	- Notify affected participants about the breach. - Provide guidance on monitoring for identity theft. - Implement stricter access control mechanisms.
8	Satisfaction survey from students at the end of a learning course or activity.	Low	- Implement secure storage and access control to authorized personnel only. - Anonymize sensitive information, when possible	- Remove or anonymize exposed data retroactively if possible. - Strengthen survey platform security.
9	Marketing data related to communication and dissemination activities.	Medium	- Restrict access to marketing databases. - Use encryption for sensitive marketing-related information.	- Monitor for phishing or spam activities using leaked data. - Reassess marketing database access policies.

Table 4: Data types, breach likelihood, mitigation and corrective measures

2.4 Retention period

The retention period for the project varies depending on the status of the applicant and the purpose of data retention:

- For beneficiaries receiving EU funding, personal data is typically retained for 10 years after the end of the year following closure of the project[2].

- For other data sets, including personal data, it is retained for up to 5 years after the end of the year following closure of the project.

3 FAIR data

3.1 Making data findable, including provisions for metadata

To ensure that the data generated during the project is findable, we will implement the following provisions:

- All data will be recorded in a predeterminate structure and with an agree format.
- 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 made available through appropriate repositories and archives to enable discovery and reuse.
- Data will be assigned unique identifiers to enable easy identification and tracking.
- Data will be stored in a structured and organized manner to enable efficient searching and browsing, appropriate metadata and keywords will also be identified for effective indexing and search.

3.2 Making data openly accessible

The following table is highlighting which data described in Table 1: Data sets overview will be made openly available. It also explains why several datasets cannot be shared because of particular reasons and, in this case, an alternative solution will be presented.

#	*Data type*	*Openly available*	*Justification*	*Alternative solution*
1	Market review of Cybersecurity sector.	Yes	Results of this analysis will be described in the project deliverable D1.1.	*(not relevant)*

[2] https://commission.europa.eu/law/law-topic/data-protection/rules-business-and-organisations/principles-gdpr/how-long-can-data-be-kept-and-it-necessary-update-it_en

#	Data type	Openly available	Justification	Alternative solution
2	Market review of Robotics sector.	Yes	Results of this analysis will be described in the project deliverable D2.1.	*(not relevant)*
3	Literature review data on Cybersecurity.	Yes	Results of this review will be described in the project deliverable D1.1.	*(not relevant)*
4	Literature review data on Robotics.	Yes	Results of this review will be described in the project deliverable D2.1.	*(not relevant)*
5	Recruitment cycle data about participants (incl. FSTP applicants)	No	The sensible data about students involved in the recruitment process of the project will not be released, in respect to GDPR and any other regulation that may apply.	Data will be pseudo-anonymized. Statistical data about the recruitment cycle and student admissions will be described in the project deliverables D4.4, D4.5, D4.6, D4.7.
6	Data of students participating to master programmes.	No	The sensible data about students participating to courses and learning activities of the project will not be released, in respect to GDPR and any other regulation that may apply.	Statistical data about the student participation to the master will be described in the project deliverables D1.2, D1.3, D1.4, D2.2, D2.3, D2.4.
7	Data on participants to self-standing modules.	No	All personal data, including contact information, regarding students, will not be make openly available, in respect to GDPR and any other regulation that may apply.	Statistical data about the student participation to the master will be described in the project deliverables D1.2, D1.3, D1.4, D2.2, D2.3, D2.4.
8	Satisfaction survey from students at the end of a learning course or activity.	No	All personal data of students, including contact information and opinion on the course quality, will not be make openly available, in respect 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 D1.2, D1.3, D1.4, D2.2, D2.3, D2.4.
9	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.	Statistical aggregated data about marketing and dissemination activities will be released in deliverables D3.2, D3.3, D3.4, D3.5.

Table 5: Data sets accessibility

The data made available, 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.

3.3 Making data interoperable

All the data shared by the project will use document standards that will make it interoperable. The data will be released with docx or xlsx file formats promoting interoperability by providing a standardized, open, and flexible way to exchange and reuse data across different systems and applications.

3.4 Increase data re-use (through clarifying licences)

To permit the wides re-use of data, all openly available project deliverables and main results will be released with a Creative Commons Attribution (CC-BY) license, unless this conflicts with the license of the some input source. 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 adequately,
- the master course, that will remain property of the producing entity, and
- the online training modules.

This data will maintain a shared ownership between the beneficiaries that have generated them. The reason for not releasing this data openly involves:

- Intellectual Property Rights (IPR) Protection: The master course may involve proprietary content or methodologies developed by the producing entity. Opening up this material could infringe on intellectual property rights, which are designed to protect the creators' or institutions' innovations and investments.
- Commercial Exploitation: If the material is intended for commercial exploitation, making it openly available could undermine the potential market value and the ability of the producing entity to recover development costs or generate revenue. This is often a consideration in projects where commercialization of results is a key objective.
- Privacy and Confidentiality: Courses may contain sensitive information, personal data, or case studies that are not suitable for open distribution due to privacy laws or confidentiality agreements. In such cases, the protection of this information takes precedence over open access.
- Quality Control and Brand Integrity: The producing entity may wish to retain control over the dissemination and use of the course materials to ensure they are used in a manner that maintains the quality, integrity, and reputation of the educational content and the institution.

4 Allocation of resources

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

1. **Personnel**: Data management will be overseen in Task 4.5 of the WP4. 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 responsible for training project personnel in data management best practices.

2. **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.
3. **Budget**: The project will allocate a budget for data management activities. The budget will also include provisions for the dissemination and sharing of data, including the use of appropriate repositories and archives.
4. **Deliverables**: This deliverable D4.2 of the project describes an initial data management plan. The project will also include deliverables for the dissemination and sharing of data.

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.

Our proposed approach for long-term data preservation involves selecting critical datasets for retention based on their potential for future research and educational use, storing them in a domain-relevant FAIR-compliant digital repository (Zenodo: https://zenodo.org/) for at least 10 years, and ensuring their accessibility through open, non-proprietary formats and comprehensive metadata, while adhering to legal and ethical standards for data sharing.

5 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. A template Consent form for collection of personal data is available in Annex 1.
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 anonymization 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.

6 Processing of personal data

Please refer to Annex 2 – Privacy policy, for a detailed description of the SPECTRO project privacy policy.

As described in Table 1: Data sets overview, the project will be collecting and processing personal data of specific participants:

- Participants applying to SPECTRO Master programmes (incl. FSTP applicants)
- Students participating to SPECTRO Master programmes
- Participants to SPECTRO self-standing modules
- Satisfaction survey from students at the end of a learning course or activity.
- Marketing data related to communication and dissemination activities (ie. An individual fill in the "contact me" form on the EITD website, an individual registers to attend meetings, workshops and other events we host and during attendance at such events)

Participants applying to SPECTRO Master Programme applicants must submit their application via the admission portal. Applicants are required to provide certain personal information to the system (i.e contact information, ID, email and postal addresses). All applicants must read and agree with EIT Digital Privacy policy and Master School Terms and Conditions and consent to allow EIT Digital to store and process their personal information. The documentation to read explains the grounds for personal data processing, the purpose for personal data collection, and the measures in place to protect personal data.

Students participating to SPECTRO Master programmes sign a Student agreement contract with the EIT Master School Office. EIT Digital provides Master School students with a management system to administer the relevant aspects of the Programme. Students are required to provide certain personal information to the system (i.e. bank details, contact information, transcript of records). The collection and management of EIT Digital Student Data is described under Article 11 of the Student Agreement Contract.

Participants to SPECTRO self-sanding modules must enrol to the Icarus AI platform to access the courses. Participants are required to provide certain personal information to the system (i.e contact information). All applicants must read and agree with the Privacy Policy to allow EIT Digital and Icarus AI to store and process their personal information. The documentation to read explains the grounds for personal data processing, the purpose for personal data collection, and the measures in place to protect personal data.

Students taking a satisfaction survey are required to provide certain personal information such as contact details (name/ surname, e-mail address, phone number); professional information (job title, organisation, field of expertise); demographics (e.g. age, gender, nationality).

Marketing data related to communication and dissemination activities: participants' personal data fall into the following caterogies: contact details (name/ surname, e-mail address, phone number); professional information (job title, organisation, field of expertise); demographics (e.g. age, gender, nationality).

EIT Digital takes reasonable security measures to protect all personal data from destruction, loss, modification or any other unauthorised processing. EIT Digital do not store personal data for longer than necessary for the purposes for which it is stored.

Any applicant or student has the right to request free access to the personal data processed by EIT Digital to request the correction or removal of their data or to request a restriction of the processing. They may also request the portability of their data and you may object to the processing of your personal data, without substantiation in the case of direct marketing, or substantiated in other cases.

When the processing of their personal data is based on their consent, they may revoke this at any time. Revocation of consent does not affect the lawfulness of the processing based on consent before withdrawal.

Requests may be redirected to privacy@eitdigital.eu.

Participants also have the right to file a complaint with the supervisory authority, which is the Commission for the Protection of Privacy. It can be reached by mail at Rue de la Presse 35, 1000 Brussels, and by e-mail at the following address: commission@privacycommission.be.

7 FSTP applicants data management

FSTP applicants' data is managed in the data set 'Recruitment cycle data about participants (incl. FSTP applicants)'. Please refer to sections 2 Data Summary and 6 Processing of personal data for details.

For beneficiaries receiving EU funding, personal data is typically retained for 10 years after the end of the year following closure of the project .

As a contractual obligation, EITD must publish FSTP beneficiary information (post-award). The result of each FSTP call and the scholarships awarded will be available on the SPECTRO webpage.

8 Other issues

Data management in the project will be performed following the European Commission's Digital Europe procedures. In particular this document represents the Data Management Plan (DMP) as requested in the program and describes the data management life cycle for the data to be collected, processed, and/or generated by the project.

The project will require collection of the KPIs and their sharing with the EU. The legal indicators for SO4 have been established in Annex II of Regulation, establishing the DIGITAL Programme. Underlying definitions and concepts of the indicators can be found in the Commission Staff Working Document "Monitoring and Evaluation Framework for the

Digital Europe Programme" (pages 24 and 25). Indicators refer to the number of persons who have received training to acquire advanced digital skills supported by the Programme, the number of enterprises, in particular SMEs, having difficulty recruiting ICT specialists (when applicable) and the number of people reporting an improved employment situation after the end of the training supported by the Programme. The submission form (KPI tab) will take the gender dimension into account and will collect, where possible, sex aggregated data on participants of the training courses and the completion rate.

References

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

[SPECTRO] http://eitdigital.eu/spectro/

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])
DPO	Data Protection Officer
EC	European Commission
EIT	European Institute of Innovation and Technology
KIC	Knowledge and Innovation Community
GA	Grant Agreement
GDPR	General Data Protection Regulation
R&S	Research and scholarship

Annex 1. Template consent form for processing of personal data

SPECTRO
SPECIALISED EDUCATION PROGRAMMES IN CYBERSECURITY AND ROBOTICS
Co-funded by the European Union

[Organisation Name] [Organisation Address] [Contact Information] [Website]

1. Purpose of Data Processing [Organisation Name] ("we", "our", "us") need to collect and keep some of your personal data in order to [insert specific purpose]. [Organisation Name] is committed to protecting your personal data in accordance with the General Data Protection Regulation (GDPR)[3]. We seek your consent to process your personal data for the following purpose(s): *[select or draft all that applies]*

- Collection and use of personal data (e.g., name, contact details, identification documents, etc.) for [specific purpose].
- Image/voice recording for [specific purpose, e.g., event documentation, marketing, training, etc.].
- [other]

2. Type of Data Collected The personal data we collect includes:

- [List of relevant data types, e.g., full name, email, phone number, photographs, video/audio recordings, etc.]

3. Legal Basis for Processing Processing of your personal data is based on your explicit consent as per Article 6(1)(a) of the GDPR. You have the right to withdraw consent at any time without affecting the lawfulness of processing based on consent before its withdrawal.

4. Data Sharing and Retention Your data may be shared with [list of third parties if applicable] strictly for the stated purposes. We will retain your data for [retention period] after which it will be securely deleted.

5. Your Rights Under GDPR, you have the right to:

- Access, correct, or erase your data.
- Restrict or object to processing.
- Withdraw consent at any time.

To exercise these rights, contact us at privacy@eitdigital.eu and [your contact details].

You also have the right to file a complaint with the supervisory authority, which is the Commission for the Protection of Privacy. It can be reached by mail at Rue de la Presse 35, 1000 Brussels, and by e-mail at the following address: commission@privacycommission.be.

[3] General Data Protection Regulation (Regulation (EU) 2016/679): https://eur-lex.europa.eu/eli/reg/2016/679/oj

6. Consent Declaration By signing below, you confirm that you have read and understood this consent form and agree to the processing of your personal data for the specified purpose(s).

Name: __________________________________
Signature: _______________________________
Date: ___________________________________

Withdrawal of Consent If you wish to withdraw consent, please contact us at [your contact details].

For Official Use Only Processed by: ____________________________
Date: ___________________________________

Annex 2. Privacy Policy

Within this Annex, the reader can find the project's overall Privacy Policy. Work Package leaders are responsible for developing any additional privacy policy needed in their tasks and activities in close collaboration with the PC.

1. Who we are

SPecialised Education programmes in CybersecuriTy and Robotics (SPECTRO) focuses on the design and delivery of two double-degree master's programmes (ISCED Level 7, 120 ECTS) and self-standing learning modules in two key digital technology areas for the future of Europe:

1. Cybersecurity
2. Robotics

The two specialised master's programmes, which will also include a minor in Innovation and Entrepreneurship, will be designed and delivered by a consortium consisting of 14 higher education institutions from 8 different countries, 2 innovative SMEs, 1 leading research centre in Information Systems and EIT Digital, a pan-European organisation with in-depth knowledge and experience in the digital skills domain.

The project partners of the SPECTRO consortium, listed below, process certain types of personal data for the purposes of the project. Each partner is responsible for the personal data they collect and process during their activities under the framework of the project:

EIT Digital
Eötvös Loránd University
University of Trento
University of Twente
University of Rennes
University of Turku
EURECOM
Babeș-Bolyai University
KTH Royal Institute of Technology
Aalto University
University of Bologna
University Côte d'Azur
Budapest University of Technology and Economics
University of the Agean
Politecnico di Bari
Evolutionary Archetypes Consulting SL
Gim Robotics

For further information, we can be contacted at spectro@eitdigital.eu

2. How we collect your personal data

We only collect the data necessary for our project's smooth implementation. We obtain personal data directly from individuals in a variety of ways, including the following cases:

- Participants applying to SPECTRO Master programmes (incl. FSTP applicants)
- Students participating to SPECTRO Master programmes
- Participants to SPECTRO self-standing modules
- Satisfaction survey from students at the end of a learning course or activity.
- Marketing data related to communication and dissemination activities (ie. An individual fill in the "contact me" form on the EITD website, an individual registers to attend meetings, workshops and other events we host and during attendance at such events)

3. What types of data we collect

Participants applying to SPECTRO Master Programme applicants must submit their application via the admission portal. Applicants are required to provide certain personal information to the system (i.e contact information, gender, nationality, ID, email and postal addresses). All applicants must read and agree with EIT Digital Privacy policy and Master School Terms and Conditions and consent to allow EIT Digital to store and process their personal information. The documentation to read explains the grounds for personal data processing, the purpose for personal data collection, and the measures in place to protect personal data.

Students participating to SPECTRO Master programmes sign a Student agreement contract with the EIT Master School Office. EIT Digital provides Master School students with a management system to administer the relevant aspects of the Programme. Students are required to provide certain personal information to the system (i.e. bank details, contact information, transcript of records). The collection and management of EIT Digital Student Data is described under Article 11 of the Student Agreement Contract.

Participants to SPECTRO self-sanding modules must enrol to the Icarus AI platform to access the courses. Participants are required to provide certain personal information to the system (i.e contact information). All applicants must read and agree with the Privacy Policy to allow EIT Digital and Icarus AI to store and process their personal information. The documentation to read explains the grounds for personal data processing, the purpose for personal data collection, and the measures in place to protect personal data.

Students taking a satisfaction survey are required to provide certain personal information such as contact details (name/ surname, e-mail address, phone number); professional information (job title, organisation, field of expertise); demographics (e.g. age, gender, nationality).

Marketing data related to communication and dissemination activities: participants' personal data fall into the following caterogies: contact details (name/ surname, e-mail address, phone number); professional information (job title, organisation, field of expertise); demographics (e.g. age, gender, nationality).

4. Bases of lawful processing

We process personal data on the following legal bases:

- Legal obligations – for processing activities required for compliance both with applicable national and European legislation as well as with the specific legal and regulatory framework of the Digital Europe Framework Programme.
- Consent – for processing activities such as organisation of meetings, workshops, other events, and dissemination of project's results.
- Contractual obligations – for processing activities such as reporting to the European Commission and complying with project's publicity obligations.

5. What do we do with your personal data

We process your personal data with the purpose of:

- Processing applications of SPECTRO students
- Disseminating our project's results to different types of stakeholders;
- Sending invitations and providing access to guests attending our meetings, events, and workshops;
- Processing online requests or queries, including responding to communications from individuals;
- Complying with contractual, legal, and regulatory obligations.

6. How we secure your personal data when we process it

We apply a personal data risk assessment process to identify, analyse, and evaluate the security risks that may threaten your personal data. Based on the results of this risk assessment, we define and apply a set of both technical and organizational measures to mitigate the above security risks. Please refer to Section 2.3 Data breach mitigation and corrective measures, for further details.

7. Do we share personal data with third parties?

Your personal data may be shared with trusted third parties to help us deliver efficient and quality services. When we do so, we ensure that recipients are contractually bound to safeguard the data we entrust to them before we share the data. We may engage with several or all of the following categories of recipients:

- Parties that support us as we provide our services (e.g., cloud-based software services such as Microsoft SharePoint);
- Our professional advisers, including lawyers, auditors, and insurers;
- Dissemination service providers (e.g., HubSpot);
- Law enforcement or other government and regulatory agencies or other third parties as required by, and in accordance with applicable law or regulation;
- The European Commission according to our relevant contractual obligations.

8. Do we transfer your personal data outside the European Economic Area?

We do not own file servers located outside the European Economic Area (EEA). However, some partners may use cloud and/or marketing services from reputable providers such as SharePoint, HubSpot, etc., situated both inside and outside the EEA. We always check that such providers comply with the relevant GDPR requirements before starting to use their services.

9. Do we use cookies?

Please consult EIT Digital website's Privacy policy directly to know more about our cookie policy.

10. Your rights

You have the following rights regarding our processing of your personal data:

- Right to withdraw consent – You can withdraw consent that you have previously given to one or more specified purposes to process your personal data. This will not affect the lawfulness of any processing carried out before you withdraw your consent.
- Right of access – You can ask us to verify whether we are processing personal data about you and if so, to have access to a copy of such data.
- Right to rectification and erasure – You can ask us to correct our records if you believe they contain incorrect or incomplete information about you or ask us to erase your personal data after you withdraw your consent to processing or when we no longer need it for the purpose it was originally collected.
- Right to restriction of processing – You can ask us to temporarily restrict our processing of your personal data if you contest the accuracy of your personal data, prefer to restrict its use rather than having us erase it, or need us to preserve it for you to establish, exercise or defend a legal claim. A temporary restriction may apply while verifying whether we have overriding legitimate grounds to process it. You can ask us to inform you before we lift that temporary processing restriction.
- Right to data portability – In some circumstances, where you have provided personal data to us, you can ask us to transmit that personal data (in a structured, commonly used, and machine-readable format) directly to another entity.
- Right to object – You can object to our use of your personal data for direct marketing purposes, including profiling or where processing has taken the form of automated decision-making. However, we may need to keep some minimal information (e.g., e-mail address) to comply with your request to cease marketing to you.
- Right to make a complaint to your local Data Protection Authority (DPA) (see https://ec.europa.eu/justice/article-29/structure/data-protection-authorities/index_en.htm) regarding any concerns you may have about our data handling practices.

To ask us to do anything of the above, you can contact us by email: privacy@eitdigital.eu. We will promptly examine your request against the relevant requirements of the laws and regulations governing privacy and personal data protection and we will answer the latest within 30 days after receiving your request. We will ask you for some kind of identification (e.g. photocopy of your identity card or passport) to avoid the non-authorized reveal of your personal data. If for reasons of the complexity of the request or a multitude of requests, we are unable to respond promptly, we will notify you within 30 days of any delay, which in no case may exceed two months from the expiration of the 30-day deadline.

11. How long do we retain personal data?

We retain personal data to provide our services, stay in contact with you and comply with applicable laws, regulations, and contractual obligations to which we are subject. Please note that we have an obligation to retain data concerning projects funded by the Digital Europe programme for up to five years after the end of the project (unless auditors request further retention). For beneficiaries receiving EU funding, personal data is typically retained for 10 years after the end of the year following closure of the project. .After the expiry of the retention period, and unless further legitimate grounds for retention arise, we will dispose of personal data in a secure manner.

12. Disclaimer of liability for third-party websites

Although our sites may contain links to third-party sites, including the sites of the SPECTRO consortium partners, we are not responsible for the privacy practices or content of these sites, and we expressly disclaim any liability for any loss or damage that may be caused by the use of these links. We do not monitor the privacy practices or the content of these sites. If you have any questions about the privacy practices of another site, you should contact the site's responsible personnel. We suggest you read the privacy policy of each website you interact with, before allowing the collection and use of your personal data. We may also provide social media features that allow you to share information on your social networks and interact with the SPECTRO project on various social media sites. The use of these social media features may result in the collection or sharing of information about you. We recommend that you check the privacy policies and regulations of the social networking sites you interact with to ensure that you understand what information may be collected, used and disclosed by these sites.

13. Children

We do not knowingly collect, use, or disclose information from children under the age of 16. If we learn that we have collected the personal information of a child under 16 we will take steps to delete the information as soon as possible. Please immediately contact us if you become aware that a child under 16 has provided us with personal information.

14. Validity of this Privacy Policy

This Privacy Policy is valid from 1/9/2023. We reserve the right to revise this Policy at any time. The current version will be always uploaded as an Annex to Deliverable 4.2. If there are critical changes in this policy or our personal data practices change significantly in the future, we will notify you by posting the changes as an Annex to Deliverable D4.2.