D5.2
Data Management Plan

Project Name	Enhancing Cross-Sectoral Collaboration in Cybersecurity in Estonia, Czechia, Lithuania, Ukraine, and the Netherlands
Project acronym	SECURE-NET
Grant agreement no.	101217315
Call	HORIZON-WIDERA-2024-TALENTS-03
Type of action	HORIZON-CSA
Project starting date	1 September 2025
Project duration	48 months
Deliverable Number	D5.2
Deliverable name	Data Management Plan
Lead Beneficiary	University of Tartu
Type	DMP
Dissemination Level	PU — Public
Work Package No	WP5
Due Date	February 2026
Submission Date	18 February 2026
Version	1

Funded by the European Union

Funded by the European Union under Grant Agreement No 101217315. Views and opinions expressed are however, those of the author(s) only and do not necessarily reflect those of the European Union or [name of the granting authority]. Neither the European Union nor the granting authority can be held responsible for them.

Editor

- Mubashar Iqbal (UTARTU)
- Raimundas Matulevičius (UTARTU)

Contributors

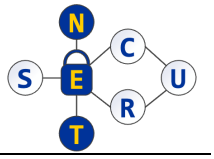
- Raimundas Matulevičius (UTARTU)
- Lukáš Daubner (UTARTU)
- Vaclav (Vashek) Matyas (MUNI)
- Hendrik Pillmann (RIA)
- Liina Kamm (CYBER)
- Kęstutis Kapočius (KTU)
- Rimantas Butleris (KTU)
- Robertas Ulinskas (ITS)
- Dimka Karastoyanova (RUG)
- Batina, L. Lejla (RUN)
- Durga Lakshmi Ramachandran (KEYS)
- Serhii Sharyn (PNU)
- Volodymyr Shcherbiak (POE)

Reviewers

- Diana Pilvar (UTARTU)
- Lukáš Daubner (UTARTU)
- Liina Kamm (CYBER)
- Serhii Sharyn (PNU)
- Volodymyr Shcherbiak (POE)

History of Changes in DMP

Version	Publication date	Change
1.0	18.02.2026	Version 1.0



SECURE-NET Consortium

Participant organization name	Short name	Country
University of Tartu	UTARTU	Estonia
Masaryk University	MUNI	Czechia
Estonian Information System Authority	RIA	Estonia
Cybernetica AS	CYBER	Estonia
Kaunas University of Technology	KTU	Lithuania
UAB IT Solutions	ITS	Lithuania
University of Groningen	RUG	Netherlands
Radboud University	RUN	Netherlands
Keysight Technologies Netherlands Riscure BV	KEYS	Netherlands
Vasyl Stefanyk Carpathian National University	PNU	Ukraine
Joint-stock company “Prykarpattyaoblenergo”	POE	Ukraine

Abbreviations

AB	-	Advisory Board
DMP	-	Data Management Plan
EC	-	European Commission
FAIR	-	Findable, Accessible, Interoperable, and Reusable
GA	-	Grant Agreement
PMT	-	Project Management Team
SC	-	Steering Committee
WP	-	Work Package

Executive Summary

This Data Management Plan (D5.2) describes how data and other research outputs generated within the SECURE-NET project are collected, managed, stored, shared, and preserved throughout the project lifecycle and beyond. The plan follows the FAIR principles and the requirements of the Grant Agreement (GA). Different data types, ranging from personal data and internal reports to publications, software, datasets, and multimedia materials, are managed according to their sensitivity and purpose. The plan ensures that non-sensitive outputs are made openly available whenever possible, while sensitive data remain protected and accessible only to authorised partners. This document will be reviewed and updated twice in M24 (D5.4) and M47 (D5.5), as needed, to reflect project progress and any new data management needs.

Table of Contents

List of Tables

List of Figures

1. Introduction

This document is deliverable D5.2 Data Management Plan (DMP). The D5.2 describes the various aspects in line with the EU-provided FAIR principles template [2] to ensure that the SECURE-NET project results are organised, secure, discoverable, and reusable.

The D5.2 provides a structured, comprehensive overview of how data and research outputs generated within the SECURE-NET project will be managed, preserved, and shared. The D5.2 is a non-sensitive document and is intended for public dissemination and serves as a reference for project partners, stakeholders, and external audiences, outlining the policies and practices that ensure compliance with the principles of Open Science and the FAIR data management framework.

The D5.2 addresses types of data generated or reused in the project, including personal data, internal reports and white papers, publications, source code and proof-of-concept implementations, presentations, workshop materials, use cases and datasets, and multimedia files. The plan supports the discoverability, accessibility, and reuse of project outputs while safeguarding sensitive information and respecting ethical, legal, and contractual obligations.

The D5.2 describes the processes and resources allocated to effective data management, including identifying responsible partners, assigning roles and responsibilities, and selecting appropriate repositories and storage platforms for long-term preservation and secure access. The DMP provides guidelines to showcase how, within the SECURE-NET project, we ensure data quality, documentation, and provenance, including the use of metadata, references, and standard formats to enhance interoperability within and across disciplines. The DMP describes how sensitive and personal data are managed, with strict access controls and ethical oversight, to ensure confidentiality and compliance with relevant legal requirements.

Additionally, the D5.2 also covers the management of other research outputs, such as source code, proof-of-concept implementation files, workshop materials, and multimedia. These outputs demonstrate the project's practical results and knowledge transfer. The plan outlines how these outputs will be documented, stored, and shared, including measures for open access where applicable. It highlights the platforms and repositories used, such as Google Drive, Zenodo, GitLab, and the SECURE-NET project website and social media channels, for disseminating presentations and multimedia content.

1.1 SECURE-NET Project

The SECURE-NET project aims to strengthen research and innovation capacities in cybersecurity across four widening countries: Estonia, Czechia, Lithuania, and Ukraine. The project focuses on addressing existing gaps in skills, collaboration, and innovation performance by supporting the development of advanced research competencies and practical expertise in cybersecurity. Through targeted activities, SECURE-NET seeks to

build a more substantial, more connected research and innovation ecosystem that supports long-term growth and excellence in these countries.

To achieve this objective, SECURE-NET promotes enhanced cross-sectoral collaboration and improved training of research and innovation talents across academia, industry, and the public sector. The project places strong emphasis on knowledge exchange, mobility, and hands-on experience, enabling researchers and practitioners to work together and learn from different environments. This approach supports the development of practical skills, strengthens cross-sector collaboration, and improves the employability and career prospects of researchers.

SECURE-NET brings together a consortium of 11 partners with complementary expertise and roles. Eight partners are based in widening countries, including three organisations from Estonia representing academia, government, and industry; two partners from Lithuania and two from Ukraine, each including one academic and one business organisation; and one academic organisation from Czechia. These partners are supported by three organisations from the Netherlands, including two academic institutions and one business partner. This balanced consortium structure ensures strong knowledge transfer, mentoring, and capacity building, supporting the project's overall goal of enhancing cybersecurity research and innovation capabilities in the participating widening countries.

1.2 Organisation of the SECURE-NET Project

The SECURE-NET project includes the Project Management Team (PMT), the Steering Committee (SC), and the Advisory Board. The PMT is responsible for the daily execution and monitoring of the SECURE-NET project's tasks and activities, while the SC provides high-level oversight and strategic decision-making. The external Advisory Board offers independent expert guidance and validation.

The SECURE-NET has developed a methodology (Fig. 1) to support the proposed cross-sectoral collaborations and to improve the training of research and innovation talent across academia, industry, and the public sector. Cross-sectoral collaborations include individual secondments of research staff from partner organisations and consortium-wide training events for research and support staff. The planned secondments and training events have been defined based on the use cases provided by non-academic business sector partners, as well as on complementary partner expertise across the various cybersecurity domains.

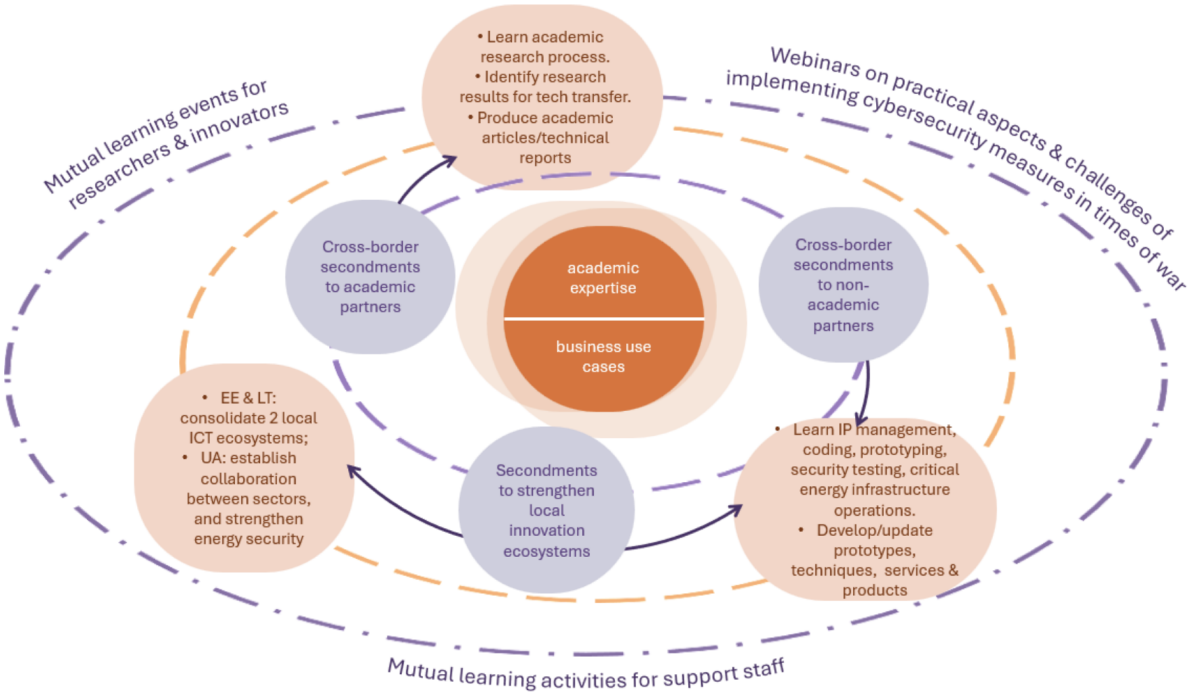


Figure 1: Overview of the SECURE-NET methodology, adapted from GA [1].

The planned SECURE-NET secondments are in line with the rules of the call HORIZON-WIDERA-2024-TALENTS-03-01: ERA Talents as follows:

- They take place between academic and non-academic beneficiaries or between two non-academic beneficiaries.
- All secondments involve at least one participant from a widening country.
- Most secondments are cross-border, except for 6 that will take place within the same country to strengthen local ecosystems, a key goal identified by partners.
- A bit more than 71% of the budget is allocated to participants from widening countries.
- All secondments take place between independent legal entities.
- Several participants' secondments are split across periods and different hosting organisations, but none exceed 24 months.
- All secondments include Personal Career Development Plans, which will also detail return-phase activities at the sending institutions.

SECURE-NET secondments are designed to support knowledge exchange and skills development through close cooperation between academic and non-academic partners. Three types of secondments are implemented in the project. These include cross-border secondments to non-academic and academic partners, as well as to strengthen local innovation ecosystems.

The content of the secondments is defined based on real use cases provided by non-academic partners, ensuring relevance to actual business and public sector needs, and on the expertise of academic partners in specific cybersecurity domains. This approach allows

secondees to gain practical experience while contributing to research, innovation, and capacity building across sectors and countries.

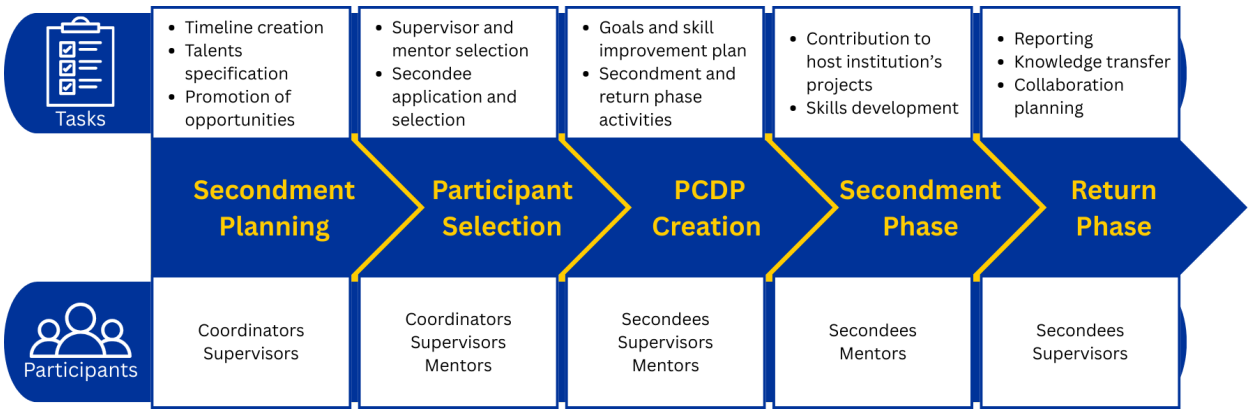


Figure 2: SECURE-NET secondment types, adapted from GA [1].

1.3 Data Management Principles

The SECURE-NET project follows clear, structured data management principles aligned with FAIR principles and the GA. The project generates seven data types across WPs, each managed according to its purpose, sensitivity, and relevance.

Personal data related to partners, secondees, mentors, and supervisors is mainly relevant to project coordination, management, and secondment activities. This data is mainly produced in WP1 and used for tasks such as project administration, secondment planning, reporting, and communication. Personal data is handled with strict confidentiality and access controls and is accessible only to authorised project partners.

Internal reports and white papers are produced mainly within WP5 and WP6 to support project management, monitoring, and reporting. These documents include progress reports, internal analyses, and summaries of activities and results. In this category, some reports (deliverables) are marked sensitive (e.g., SEN in the GA), intended for internal use and reporting only, and stored in secure, shared environments. The non-sensitive (e.g., PU in the GA) reports (deliverables) are available publicly.

Publications, including journal articles, conference papers, and workshop contributions, are mainly linked to WP2 and WP4. These outputs present the scientific and technical results of the project and contribute to knowledge sharing within the research and innovation community.

The **implementation and source code** are mainly relevant to WP2 and focus on the practical outcomes of the research, including prototypes, proof-of-concept implementations, and technical tools. This data supports experimentation, validation of research ideas, and knowledge transfer. According to the GA open science principles, this data will be shared publicly when possible.

Presentations and workshop materials are produced mainly in WP1 and WP3 and support learning events, training activities, workshops, and dissemination. These materials are used to present project progress, research results, and secondment outcomes to partners, stakeholders, and external audiences. This material will be publicly available.

Use cases, experimentation results, and datasets are mainly associated with WP2 and WP5. They are based on real-world problems and scenarios provided by non-academic partners and are used to test, validate, and demonstrate research results. These data types help ensure that the project responds to real business and societal needs. According to the GA open science principles, this data will be shared publicly when possible.

Multimedia data, such as videos, audio recordings, and pictures, is mainly linked to WP2, WP3, and WP4. This data is used for communication, dissemination, training, and visibility purposes, including showcasing project activities, events, and results. This material will be publicly available.

Across WPs, the SECURE-NET project applies common data management principles. These include using standard, widely supported formats, assigning clear data management responsibilities, ensuring data quality through reviews and validation, and applying appropriate security measures.

Table 1: Data types and relevance to the work packages

#	Data type	WP1	WP2	WP3	WP4	WP5	WP6
1	Personal data (related to partners, secondees, and mentors)	■					
2	Internal reports and white papers					■	■
3	Publications (articles in journals, conferences, and workshops)		■		■		
4	Implementation and source code		■				
5	Presentations and workshop materials			■			
6	Use cases, experimentation results, and datasets		■				
7	Multimedia data (video, audio, pictures)		■	■	■		

We define a clear folder structure to ensure documents and data are stored in an organised manner. GitLab (Figure 3a) is used for storing submitted deliverables and secondment-related reports and data, with controlled access. Google Drive (Figure 3b) is used as a shared working space for collaboration, communication materials, and meeting documents. This structure helps partners easily find documents, avoid duplication, and ensure proper version control and access management. The other platforms, such as Zenodo, research

publishers, and code repositories, use their own internal folders and organisational structures to manage and store data. Zenodo will be used to store and share the project's publications in Open Access mode: https://zenodo.org/communities/secure-net.

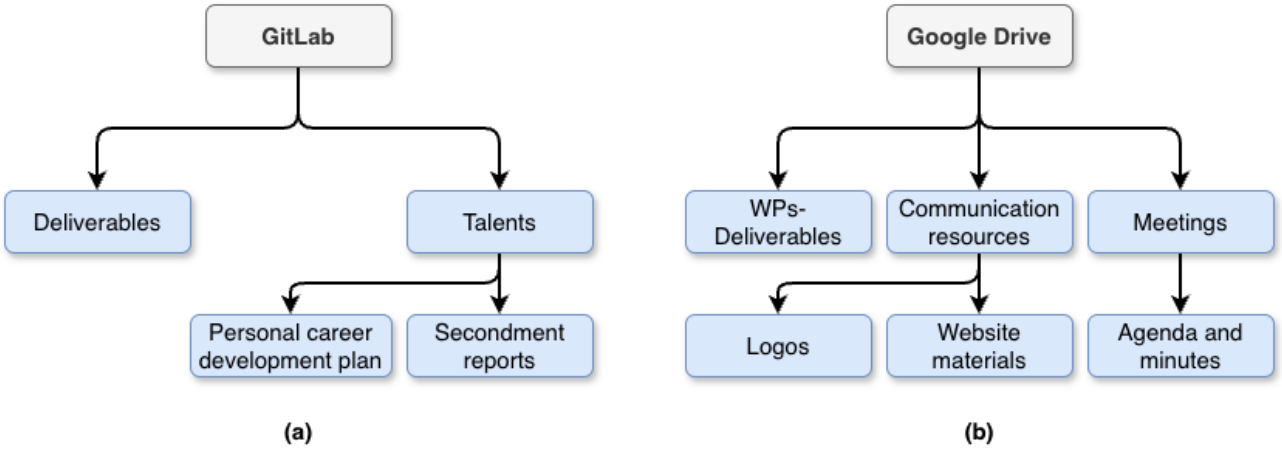


Figure 3: Folder structure for data organisation in the SECURE-NET project.

2. Data Summary

2.1 Re-use of existing data

Will you re-use any existing data, and what will you re-use it for? State the reasons if re-use of any existing data has been considered but discarded.

The existing data will be reused where this supports the project objectives, e.g., WP2, but with clear limits. We will not reuse personal or multimedia data unless individuals involved have given explicit consent. Also, any personal data used for communication or dissemination purposes (such as text, photos, or videos) will only be used with prior informed consent, for instance, during WP4 activities. However, we may reuse non-personal data in several cases. This includes existing datasets and source code, white papers, publications, experiments, proof-of-concept implementations, and case studies. This data will be determined and reused during secondments (e.g., WP2). However, the details on which datasets and source code will be reused will be specified in the updated Data Management Plans for the D5.4 and D5.5 deliverables. Additionally, existing scientific publications may be reused as background and related work in publications and presentations, as in WP2 and WP4. All reused data will be appropriately acknowledged and referenced.

2.2 Data types and formats

What types and formats of data will the project generate or re-use?

The SECURE-NET project will generate and re-use a wide range of data types and formats. These include text and document formats such as PDF and DOCX, spreadsheets like XLSX and CSV, and presentation files such as PPTX. Structured data will be stored in tables, and technical outputs will include source code and related files, which may be shared in compressed formats (e.g., ZIP). For communication and dissemination activities, multimedia formats such as MP4, MOV, JPEG, and GIF may be used.

The internal reports should follow the below-defined naming convention:

- Month-Document_Type-Deliverable-Project_Acronym-GA_Number-Deliverable_Name
    - Month = Deliverable month, e.g., M08
    - Document _Type = The assigned document type from the GA, e.g., R = Report
    - Deliverable = The assigned deliverable ID from the GA, e.g., D5.2
    - Project_Acronym = SECURE-NET
    - GA_Number = Grant agreement number, e.g., 101217315
    - Deliverable_Name = The assigned deliverable name from the GA, e.g., Data Management Plan
- *Example: M06-DMP-D5-2-SECURE-NET-101217315-Data-Management-Plan*

The Personal Career Development Plans (PCDPs) shall follow this defined naming convention:

- *Document_Type-Talent_Lablel-Talent_Number*
    - *Document_Type = PCDP*
    - *Talent_Lablel = TALENT*
    - *Talent_Number = The talent number (1-31), e.g., 12.*
- *Example: PCDP-TALENT-1*

The talent applications and related documentation shall follow this defined naming convention:

- *Document_Type-Talent_Lablel-Talent_Number-Applicant_Number-Application_Document*
    - *Document_Type = PCDP*
    - *Talent_Lablel = TALENT*
    - *Talent_Number = The talent number (1-31), e.g., 12.*
    - *Applicant_Number = Applicant number for the talent, e.g., A12*
    - *Application_Document = Application document (Application, CV, Motivation-Letter, Scoring), e.g., Motivation-Letter*
- *Example: APPLICATION-TALENT-1-A1-Application*
- *Example: APPLICATION-TALENT-1-A1-CV*
- *Example: APPLICATION-TALENT-1-A1-Motivation-Letter*
- *Example: APPLICATION-TALENT-1-A1-Scoring*

The post-secondment reports shall follow this defined naming convention:

- *Document_Type-Talent_Lablel-Talent_Number-Secondment_Number-Report_Type*
  - *Document_Type = PCDP*
  - *Talent_Lablel = TALENT*
  - *Talent_Number = The talent number (1-31), e.g., 12.*
  - *Secondment_Number = The secondment number for the talent (1, 2), e.g., 1*
  - *Report_Type = Type of the report as per the Secondment Strategy (Self = Post-Secondment Self-Evaluation Report, Self-Year = One-Year Self-Evaluation Report, Mentor = Performance Evaluation Report (Mentor), Supervisor = Performance Evaluation Report (Supervisor)), e.g., Self*
- *Example: SECONDMENT-REPORT-TALENT-1-1-Self*
- *Example: SECONDMENT-REPORT-TALENT-1-1-Self-Year*
- *Example: SECONDMENT-REPORT-TALENT-1-1-Mentor*
- *Example: SECONDMENT-REPORT-TALENT-1-1-Supervisor*

Table 2: Data types and formats according to the work packages

WP	Data type	Data format
1	Personal data	Lists and tables (e.g., .xlsx, .csv, .docx)
2	Publications (articles in journals, conferences, and workshops) Implementation and source code Use cases, experimentation results, and datasets Multimedia data (video, audio, pictures)	.docx, .pdf, .txt, mp4, .mov, .wav, .jpeg, .png, .svg, .csv, .json, .git, .zip The source code files will have data formats (i.e., extensions) based on the programming language used, e.g., .py for Python code and .html for hypertext markup language (HTML)-based web pages.
3	Presentations and workshop materials Multimedia data (video, audio, pictures)	.pptx, .pdf
4	Publications (articles in journals, conferences, and workshops) Multimedia data (video, audio, pictures)	.docx, .pdf, mp4, .mov, .jpeg, .png, .svg
5	Internal reports and white papers	.docx, .pdf
6	Internal reports and white papers	.docx, .pdf

2.3 Purpose of reused or generated data

What is the purpose of the data generation or re-use, and its relation to the objectives of the project?

The purpose of data generation and re-use in the SECURE-NET project is linked to achieving the objectives defined in the Grant Agreement (GA). We will collect and use personal data only where necessary to manage the project. This includes selecting suitable talents, defining and managing secondments, and identifying mentors and supervisors. This data supports the implementation of project activities. Internal reports and white papers are generated to support knowledge sharing among partners, monitor and report project progress, and document the results of learning events and secondments. These outputs help ensure coordination, transparency, and effective project management. Public-facing data, such as publications, presentations, and communication materials, is used to increase the visibility and international profile of the partners and to inform the broader public about the SECURE-NET project's activities and results. Moreover, technical data such as source code and proof-of-concept implementations is generated (or reused) to demonstrate the practical outcomes of research carried out during secondments. This supports the project's goal of transferring knowledge and showing real-world impact, in line with the objectives set out in the GA.

2.4 Data size

What is the expected size of the data that you intend to generate or reuse?

The expected size of the data generated or reused in the project varies by data type; however, we have included the expected sizes in Table 3. For instance, personal data will be limited in size and will mainly consist of three small tables containing information about the Project Management Team, Steering Committee, and Advisory Board. In addition, there will be short project management and secondment planning documents of around 5-10 pages. Internal reports and publications are expected to range from about 10 to 100 pages, depending on their purpose and format. Presentation materials typically contain 10-50 slides. The total volume of data generated and reused during the SECURE-NET project is expected to range from several megabytes to a few gigabytes, including documents, presentations, code, and multimedia files (diagrams, pictures, audios, and videos). The exact size of the data will be specified in the updated DMP in the D5.4 and D5.5 deliverables, using the following Table 3.

2.5 Data origin

What is the origin/provenance of the data, either generated or reused?

Personal data originates directly from individuals involved in the project, including the SECURE-NET project stakeholders, secondees, mentors, and supervisors. Additional personal data is collected from work package (WP) leads, stakeholders, and project partners when needed for project management, coordination, and reporting. Internal reports and

white papers are based on information generated through periodic meetings, questionnaires, and activities carried out within WP1-WP6, as well as through secondment activities. This data is mainly collected and compiled by WP leads, secondees, and secondment organisers. Publications, presentations, proof-of-concept implementation code, use cases, datasets, and multimedia data originate from research and development activities carried out during the secondments. This type of data will be generated by literature analysis, experimental work, validation of results, and collaborative research conducted by secondees and other involved stakeholders.

Table 3: Data size and storage location according to the produced data type

#	Data type	Size	Storage location
1	Personal data (related to partners, secondees, and mentors)	3 tables 5-10 pages (secondment planning document)	GitLab
2	Internal reports and white papers	10-100 pages	GitLab
3	Publications (articles in journals, conferences, and workshops)	10-100 pages	Zenodo and research publishers
4	Implementation and source code	Megabytes (size not yet known)	GitHub, GitLab
5	Presentations and workshop materials	10-50 slides	Project website, social media pages
6	Use cases, experimentation results, and datasets	10-100 pages or CSV for experiment results and datasets (size not yet known)	Zenodo and research publishers
7	Multimedia data (video, audio, pictures)	Megabytes to gigabytes	Project website, social media pages

2.6 Data utility outside the project

To whom might your data be useful ('data utility'), outside your project?

The usefulness of the data outside the project depends on the data type. For instance, personal data will not be used outside the project and will remain restricted to internal project needs only. Internal reports marked as sensitive in the GA are mainly for internal use and will not be shared externally. However, selected results and insights summarised in white papers and official project deliverables may be helpful to external audiences, including

researchers, the general public, companies, and funding institutions. We will ensure that any external use is subject to the rules set out in the GA. Publications, presentations, use cases, datasets, source code, proof-of-concept implementations, and multimedia files (non-sensitive, e.g., presentation recording) may be helpful to IT experts, the scientific community, companies, and other stakeholders for training, research, and development, where sharing is allowed and does not conflict with intellectual property or contractual obligations. The specific reuse value of this data will be clearer in the updated Data Management Plan in D5.4 and D5.5 deliverables.

3. FAIR Data

3.1 Making data findable, including provisions for metadata

3.1.1 Persistent identifier

Will data be identified by a persistent identifier?

The use of persistent identifiers will depend on the type of data. We will not assign persistent identifiers to internal reports and working documents. These documents will be managed using standard project naming and versioning practices. However, research publications and other research outputs, such as datasets and use cases, will be assigned persistent identifiers, such as DOIs (digital object identifiers), via platforms like Zenodo and scientific peer-reviewed research publishers.

3.1.2 Meta and its standards

Will rich metadata be provided to allow discovery? What metadata will be created? What disciplinary or general standards will be followed? In case metadata standards do not exist in your discipline, please outline what type of metadata will be created and how.

Yes, rich metadata will be provided for publicly shared data, especially for publications and research outputs. For instance, platforms such as Zenodo and scientific research publishers that follow the DataCite Metadata Schema will automatically generate and manage structured metadata in accordance with well-established standards. This metadata will typically include the title, abstract, authors, affiliations, abstract, keywords, publication date, DOI, licensing information, and other details (see Table 4). This metadata is widely used in the research community and supports discovery, citation, and reuse. Additionally, if experimental results or datasets are published alongside a research publication, they will also be described using the structured metadata provided by Zenodo and the research publisher. This ensures that the data can be found, understood, and linked to the related publications, even when no discipline-specific metadata standard is required.

Table 4: The data platforms and management of associated metadata

#	Platform	Metadata
1	GitLab, GitHub, and other code repositories	• Project title • About • Date (yyyy-mm-dd) • Revision/commit • Releases • Tags • Collaborator • Comment
3	Zenodo and publishers	• Title • Abstract • Keywords • DOI • Type (publication, dataset, use case, etc.) • Publication date (yyyy-mm-dd) • Modification date (yyyy-mm-dd) • Author(s) • Affiliation(s) • ORCID (if applicable/available) • License (if applicable/available) • Version • Volume/Issue/Pages • Size • Language • Publisher
5	Website and social media pages	• Title • Content • Attachment • Type (text, image, video, poll, etc.) • Post date (yyyy-mm-dd) • Author • Language • Tags and keywords • Mentions • Reactions • Shares/reposts

3.1.3 Keywords

Will search keywords be provided in the metadata to optimise the likelihood of discovery and potential reuse?

Yes, search keywords will be provided where possible to improve discovery and potential reuse (see Table 4). For publications, search keywords are usually included in the metadata as part of the publisher or Zenodo platform requirements. These keywords help make the publications easier to find through search engines and scientific databases. For source code and proof-of-concept implementations, keywords or tags may be added in code repositories when the platform supports this feature, to improve visibility and reuse by other users.

3.1.4 Indexing

Will metadata be provided in a way that allows it to be harvested and indexed?

Metadata will be structured and managed according to the formats in Table 4 to enable harvesting and indexing where possible. While internal reports, presentations, and workshop materials may not be fully harvestable because they are published on the project website and social media pages that do not support indexing. Research publications will be indexed in major scientific databases (e.g., Elsevier, IEEE Explore, ACM, Springer Nature, etc.), libraries, and literature search engines, including SCOPUS, Google Scholar, Web of Science, etc. The more specific indexing list will be provided in the updated Data Management Plan in D5.4 and D5.5 deliverables.

3.2 Making data accessible

3.2.1 Repository

Will the data be deposited in a trusted repository?

Data will be deposited and managed in trusted repositories based on their type and sensitivity. Personal data and the final versions of sensitive internal reports, such as D1.1, D1.2, D1.3, D2.1, D2.2, D2.4, D3.2, D3.3, D4.3, D4.5, D5.1, D5.3, and D6.1, will be stored on the UTARTU-managed GitLab platform with restricted access to ensure confidentiality and security. Internal project files (non-sensitive working documents) will be maintained on UTARTU-managed Google Drive[1], with access granted only to authorised personnel through partner-managed email accounts. Research publications will be made available through publisher platforms and deposited in Zenodo. Presentation and workshop materials will be shared publicly on the SECURE-NET project website and relevant social media channels when appropriate. The source code and proof-of-concept implementations will be stored in partner-managed repositories, such as GitLab and GitHub. The non-sensitive data will be made available under the CC-BY license. However, research publishers may have different licensing based on their publication policies.

[1] From UTARTU helpdesk: UTARTU-managed Google Drive data region is set to Europe in the Google Workspace administration settings. This setting applies to all users holding a Google Workspace for Education Standard license. According to Google's official documentation, selecting the Europe region means that the corresponding customer data is stored in European data centers (see https://support.google.com/a/answer/14310028?hl=en).

Have you explored appropriate arrangements with the identified repository for depositing your data?

Yes, UTARTU-managed Google Drive will serve as a working shared repository for internal project files. At the same time, GitLab will be used to store personal data and the final version of sensitive reports with controlled access. Publications will be deposited in Zenodo to ensure long-term preservation, indexing, and discoverability. Presentation and workshop materials, as well as multimedia content, will be shared through the project's website and, where relevant, on social media platforms such as LinkedIn and Facebook to reach broader audiences and communicate project results effectively.

Does the repository ensure that the data is assigned an identifier? Will the repository resolve the identifier to a digital object?

The project's repositories provide unique identifiers for the data, where applicable. Internal reports stored on GitLab and Google Drive will have URI-based identifiers, while the project website and social media posts will not receive formal identifiers. Publications will be assigned persistent identifiers (e.g., DOIs) by the research publishers and Zenodo. These unique identifiers for different data in the SECURE-NET project ensure that these digital objects can be reliably cited, accessed, and tracked over time.

3.2.2 Data

Will all data be made openly available? If specific datasets cannot be shared (or need to be shared under restricted access conditions), explain why, clearly separating legal and contractual reasons from intentional restrictions. Note that in multi-beneficiary projects, it is also possible for specific beneficiaries to keep their data closed if opening it would go against their legitimate interests or other constraints as per the Grant Agreement.

Not all data generated by the project will be openly available. For instance, personal data and sensitive internal reports will remain restricted due to privacy, legal, and GA requirements. White papers, presentations, and multimedia files (non-sensitive content only) will be shared publicly through Zenodo, the project website, and social media channels. Research publications, use cases, and datasets will be made openly available in line with the EU Open Science Initiative, providing unrestricted access where possible. The source code and proof-of-concept implementations will be shared by partners' managed repositories, enabling reuse while respecting intellectual property and partner constraints.

If an embargo is applied to give time to publish or seek protection of the intellectual property (e.g., patents), specify why and how long this will apply, bearing in mind that research data should be made available as soon as possible.

Embargoes are generally not expected for data generated within the SECURE-NET project. All data will be shared as soon as possible, in line with the project's goals of transparency,

knowledge sharing, and open access, unless specific intellectual property or contractual requirements necessitate temporary restrictions.

Will the data be accessible via a free, standardised access protocol?

Data accessibility will depend on its type and sensitivity. Personal data and sensitive internal reports will be accessible only to authorised personnel. Research publications will be accessible through standard protocols (OAI-PMH, REST) provided by publishers and Zenodo. White papers, presentations, and multimedia materials will also be made available via standard web access protocols (https, sftp).

If there are restrictions on use, how will access to the data be provided, both during and after the project?

Access to restricted data will be managed both during and after the project. We ensure that the personal data and sensitive internal reports stored on GitLab are accessible only to authorised personnel, with permissions controlled by the UTARTU (i.e., WP5 Lead). Similarly, permissions controlled by the UTARTU (i.e., WP5 Lead) will grant access to the internal working repository on Google Drive based on partner-provided email addresses. This will ensure that only approved users can view or edit the data while maintaining security and compliance with project and legal requirements.

How will the identity of the person accessing the data be ascertained?

The identity of individuals accessing the data will be verified through platform-specific access controls. For data stored on GitLab, user accounts are linked to email addresses, and permissions are assigned to ensure that only authorised personnel can access the information. Similarly, access to files on UTARTU-managed Google Drive is controlled through the defined user permissions associated with partner-provided email accounts. However, the publicly available outputs will not be tracked.

Is there a need for a data access committee (e.g., to evaluate/approve access requests to personal/sensitive data)?

No

3.2.3 Metadata

Will metadata be made openly available and licensed under a public domain dedication CC0, as per the Grant Agreement? If not, please clarify why. Will the metadata contain information that enables the user to access the data?

Metadata for the SECURE-NET project data will generally be made openly available in accordance with the policies of the publishers, the Zenodo platform, the project website, and the project's social media pages. Metadata will include information necessary to locate and access the corresponding data. The platforms we used to publish different data (e.g.,

Zenodo, researcher publishers, social media pages, and websites) will manage metadata in the format defined in Table 4. However, metadata for personal data and sensitive internal reports will not be openly shared to protect privacy and comply with legal and GA requirements. The non-sensitive data will be made available under the CC-BY license. However, research publishers may have different licensing based on their publication policies. Code repositories can use licenses (e.g., GNU, MIT, Apache licenses, etc.).

> *How long will the data remain available and findable? Will metadata be guaranteed to remain available after the data is no longer available?*

The data and its metadata will remain available and findable for at least 5 years after the end of the SECURE-NET project, in line with the GA requirements. However, the research publications will remain accessible for as long as supported by the Zenodo platform and the respective research publishers. Social media posts and project website materials will also remain available as long as the platforms continue to host them. Metadata for all publicly shared data will continue to provide access information, even if the original data becomes unavailable.

> *Will documentation or references to any software needed to access or read the data be included? Will it be possible to include the relevant software (e.g., in open-source code)?*

No special software will be required to access or read the project data. Standard formats such as PDF, DOCX, and PPTX will be used for documents and presentations, ensuring compatibility with commonly available tools. The project website, managed using WordPress by WP4, does not require partners to install or run any software; all users can access and interact with the site through a standard web browser. The documentation for the proof-of-concept implementation and source code will be provided via code comments and README files in the code repositories used.

3.3 Making data interoperable

> *What data and metadata vocabularies, standards, formats, or methodologies will you follow to make your data interoperable to allow data exchange and re-use within and across disciplines? Will you follow community-endorsed interoperability best practices? Which ones?*

Interoperability of the project data will primarily be ensured through the standards and practices provided by the research publishers, Zenodo, or platforms hosting the data. Research publications will follow the formats listed in Table 2 and use HTTP-accessible files for web-based content that are compatible across systems and disciplines. By using these standard formats and platform-supported metadata as defined in Table 4, the data can be exchanged, accessed, and reused easily, in line with established community practices for discoverability and interoperability.

In case it is unavoidable that you use uncommon or generate project-specific ontologies or vocabularies, will you provide mappings to more commonly used ontologies? Will you openly publish the generated ontologies or vocabularies to allow reuse, refinement, or extension?

In the SECURE-NET project, we will not use uncommon ontologies or vocabularies, nor will we create them.

Will your data include qualified references to other data (e.g., other data from your project, or datasets from previous research)?

Yes, the SECURE-NET project data will include qualified references to other relevant data where appropriate. For instance, the personal data may include links provided by participants in CVs or profiles. Research publications will follow standard citation practices to reference previous research, datasets, or related work. More generally, references may also point to project deliverables, activities, media, and other resources such as articles, datasets, or open-source libraries.

3.4 Increase data re-use

How will you provide documentation needed to validate data analysis and facilitate data re-use (e.g., readme files with information on methodology, codebooks, data cleaning, analyses, variable definitions, units of measurement, etc.)?

Within the SECURE-NET project, we will provide documentation to validate data analysis and support reuse in several ways depending on the type of data. For instance, for research publications and datasets, documentation will follow the requirements and standards set by Zenodo and research publishers (e.g., see the metadata structure in Table 4), ensuring that methods, sources, and relevant details are clearly described. Proof-of-concept implementations and source code will include manuals, readme files, license, and in-code comments to explain functionality and usage. Furthermore, where applicable, additional documentation may be provided as appendices or direct references to support reproducibility and proper understanding of the data.

Will your data be made freely available in the public domain to permit the widest re-use possible? Will your data be licensed using standard reuse licenses, in line with the obligations set out in the Grant Agreement?

The project will make data freely available in the public domain whenever possible, in line with the GA under CC-BY license. Non-sensitive deliverables and materials will be shared on the project website, and multimedia content will be accessible through the website and social media channels. Research publications will be made openly available whenever permitted by the publisher, prioritising Open Access. Proof-of-concept implementation and datasets will aim for maximum public availability and reuse, with open-source code prioritised for preservation and sharing under licenses such as the GNU, MIT, Apache, etc

licenses. In cases where data is sensitive or the code cannot be openly released, internal partner policies will govern access and use.

Will the data produced in the project be usable by third parties, in particular after the end of the project?

Yes, the data produced in the project will be usable by third parties, particularly for non-sensitive results and materials. These outputs, including research publications, datasets, and source code, will be shared publicly through the project website, open-access repositories, and code repositories. They are expected to remain accessible after the end of the project, ensuring continued availability in line with the SECURE-NET project's obligations and open science principles.

Will the data's provenance be thoroughly documented in accordance with the appropriate standards?

For personal data and implementations, provenance will be tracked using standard features of source code repositories, such as git commits (version control), ensuring a clear history of changes and contributions. For reports, research publications, and presentations, authorship will be clearly indicated, and references to other data sources will be included to provide context and traceability. For example, in Google Drive, we will use manual version control by checking the history and annotating the document, like v1.0; 1.2. Citations and source links will be tracked where necessary to maintain transparency and reproducibility.

Describe all relevant data quality assurance processes.

In the SECURE-NET project, we don't envision specific quality assurance processes. However, quality will be assessed through various means; for example, research publications will be reviewed by international peer-review committees to verify their validity and reliability. Source code and proof-of-concept implementations will follow testing and validation to ensure correct functionality and usability. Internal checks by project partners will further support the reliability and integrity of reports, datasets, and other materials. The quality assurance criteria for datasets will be defined during the secondments and documented in the updated DMP, as part of the D5.4 and D5.5 deliverables.

In line with the FAIR principles, DMPs should also address research outputs beyond data and carefully consider resource allocation, data security, and ethical considerations.

In addition to following the FAIR principles, the project will carefully address research outputs beyond data, including reports, research publications, presentations, multimedia, and source code. Resources will be allocated to support data management, storage, archiving, and dissemination activities. Ethical aspects, particularly concerning personal data and sensitive information, will be strictly observed, ensuring compliance with consent, privacy, and legal requirements. Data security measures will be applied across all outputs, including secure storage, controlled access, regular backups, and adherence to repository

and platform policies, to protect the integrity, confidentiality, and availability of the project's materials.

4. Other Research Outputs

> *In addition to data management, beneficiaries should also plan for the management of other research outputs that may be generated or reused throughout their projects. Such outputs can be either digital (e.g., software, workflows, protocols, models, etc.) or physical (e.g., new materials, antibodies, reagents, samples, etc.).*

As previously discussed, the management of the SECURE-NET project outputs, including source code, documentation, and publications, is addressed in the DMP to ensure proper organisation, storage, and accessibility, in accordance with GA.

> *Beneficiaries should consider which of the questions pertaining to FAIR data above can apply to the management of other research outputs and should strive to provide sufficient detail on how their research outputs will be managed and shared, or made available for re-use, in line with the FAIR principles.*

Research outputs from the project, including the DMP itself, are managed to ensure proper availability, sharing, and potential reuse. Their management follows FAIR principles where applicable, addressing organisation, accessibility, and documentation to support discoverability and reuse.

5. Allocation of Resources

> *What will the costs be for making data or other research outputs FAIR in your project (e.g., direct and indirect costs related to storage, archiving, re-use, security, etc.)?*

The costs of making data and other research outputs FAIR are included in the overall project budget and covered as part of the planned project activities, including storage, archiving, security, and dissemination.

> *How will these be covered? Note that costs related to research data/output management are eligible as part of the Horizon Europe grant (if compliant with the Grant Agreement conditions)*

The costs for managing research data and other outputs will be covered through the SECURE-NET project budget, with each responsible partner allocated funding in line with the GA conditions.

> *Who will be responsible for data management in your project?*

Data management in the project will be primarily overseen by the UTARTU (i.e., WP5 Lead), with support from other partners. Responsibility for specific data will depend on its type and

involve the project coordinator, WP leads, secondees, mentors, and supervisors, as appropriate.

> *How will long-term preservation be ensured? Discuss the necessary resources to accomplish this (costs and potential value, who decides and how, what data will be kept, and for how long).*

Long-term preservation will focus on maintaining only the data necessary for project management, secondment coordination, and reporting. Personal data will be retained securely for the duration required by the project. Decisions on what to preserve and for how long will follow project-defined policies in accordance with the GA [1], with resources allocated through the project budget to ensure secure storage, controlled access, and compliance with legal and ethical requirements. The more specific details related to costs and potential value will be determined during project activities and updated in the DMP in the D5.4 and D5.5 deliverables. Additionally, the partners will agree on where data will be kept and for how long, in accordance with the GA.

6. Data Security

> *What provisions are or will be in place for data security (including data recovery as well as secure storage/archiving and transfer of sensitive data)?*

Sensitive data will be stored securely with controlled access, using individual permissions linked to authorised email accounts. Backup copies will be maintained to ensure data recovery and prevent loss. Internal working documents and reports will be stored in the shared UTARTU-managed Google Drive space. At the same time, the security of other project data (e.g., code, implementations, use cases, datasets, etc) will be managed by the respective project partners.

For data recovery, regular backup measures are in place. For instance, the project website and its related data are backed up weekly. UTARTU-managed Google Drive provides built-in version history and file recovery, allowing us to restore previous versions or recover deleted files if needed. UTARTU-managed GitLab also maintains version control and backup mechanisms, allowing us to restore the project structure and files in case of accidental deletion, such as if someone mistakenly removes the main project folder. Access rights are limited to authorised users to reduce the risk of such incidents.
Regarding partners from Ukraine, we recognise that they may require additional protection due to the current security situation. If sensitive information were leaked, it could potentially cause harm. For this reason, the project applies extra care when handling data related to Ukrainian partners. Sensitive documents are clearly marked, access is restricted, and personal information is minimised. Where possible, participants are anonymised in reports and research outputs. For details, we refer to the deliverable D6.1.

> *Will the data be safely stored in trusted repositories for long-term preservation and curation?*

Project data will be safely stored in trusted repositories, depending on its type. Personal data will be kept on the UTARTU-managed GitLab repository, ensuring secure access. Research publications will be deposited in Zenodo and on publisher platforms, providing reliable long-term storage and discoverability. Internal reports and mutual working documents will be stored in the shared UTARTU-managed Google Drive space, accessible only to authorised project personnel.

7. Ethics

> *Are there, or could there be, any ethics or legal issues that can have an impact on data sharing? These can also be discussed in the context of the ethics review. If relevant, include references to ethics deliverables and the ethics chapter in the Description of the Action (DoA).*

We will carefully observe ethical and legal considerations in the SECURE-NET project, in accordance with the European Code of Conduct for Research Integrity [3].

Personal data will remain confidential and accessible only to authorised SECURE-NET project partners, in accordance with standards (e.g., GDPR) and the project's established ethics procedures. Any unexpected ethical or legal issues that arise will be addressed in accordance with the procedures of the affected project partners to ensure compliance with ethical, legal, and contractual requirements. Any ethics or legal issues that emerge during the project will be reported in the updated DMP in D5.4 and D5.5 deliverables. Additionally, now, we don't know any specific intellectual property-related matters. However, they might come later, which we can similarly report in the updated DMP in D5.4 and D5.5 deliverables.

For security and policy reasons, some PCDPs shall be anonymised, with names available only on a need-to-know basis (e.g., host institution mentor). The cases are secondees going on secondment to or from Ukraine shall have their PCDPs anonymised for security reasons. Similarly, due to the organisation's policy, secondees from RIA shall have anonymous PCDPs. A contact email for both cases shall be the institution's coordinator.

We explicitly list the roles (e.g., controllers/processors), lawful bases, retention schedules, and access controls for all secondment-related personal data (Table 5).

We confirm the minimal administrative and safety dossier as already described in the D6.1 follow-up: name, role/organisation, work contacts, proof-of-insurance flag, induction/training confirmations, attendance timestamps, and factual alert/all-clear timestamps if recorded. We do not process special-category data, we do not use geotracking, and we avoid private location data.

As iterated above in different sections, the SECURE-NET project follows responsible security and a dual-use protocol to ensure that it does not disclose sensitive details and that all publications, demos, training materials, and repositories undergo a pre-publication sensitivity review. Vulnerabilities are handled through coordinated disclosure, sensitive

technical details are removed or generalised, and access to materials is controlled, logged, and regularly reviewed.

For further details, we refer to the Ethics deliverable D6.1.

Table 5: The SECURE-NET project data handling and management according to the roles, lawful bases, retention schedule, and access control

	Personal data (related to partners, secondees, and mentors)	Internal reports and white papers	Publications (articles in journals, conferences, and workshops)	Implementation and source code	Presentations and workshop materials	Use cases, experimentation results, and datasets	Multimedia data (video, audio, pictures)
Controller	UTARTU	UTARTU	UTARTU, Zenodo, and research publishers	The data producer	The data producer	The data producer	The data producer
Processor	UTARTU	UTARTU	UTARTU, Zenodo, and research publishers	The data producer and project partners	The data producer and project partners	The data producer and project partners	The data producer and project partners
Lawful bases	GA	GA	GA	GA	GA	GA	GA
Retention schedules	5 years after the project	5 years after the project	Until the storage platform is live	Until the storage platform is live	Until the storage platform is live	Until the storage platform is live	Until the storage platform is live
Access control	UTARTU (r, w) Partners (r)	UTARTU (r, w) Partners (r)	Open	Open	Open	Open	Open

Legend: r – read; w- write.

Will informed consent for data sharing and long-term preservation be included in questionnaires dealing with personal data?

For personal data, formal informed consent for long-term data sharing is not systematically collected. However, all participants are made aware that their data will be shared, processed, and stored within the project with authorised stakeholders of the SECURE-NET project. Consent to share within the project and to retain data during the project period will be obtained from individuals when necessary, to ensure transparency and compliance with ethical standards.

8. Other Issues

Do you, or will you, make use of other national/funder/sectorial/departmental procedures for data management? If yes, which ones (please list and briefly describe them)?

No

9. Concluding Remarks

The D5.2 provides a clear, structured framework for the responsible handling of data and research outputs generated in the SECURE-NET project. It ensures that data is managed in a secure, ethical, and transparent manner, while maximising its value through reuse, sharing, and long-term preservation where appropriate. By defining roles, repositories, access conditions, and quality assurance measures, the plan supports effective collaboration among partners and compliance with FAIR principles and Horizon Europe requirements. As a living document, D5.2 will continue to guide data management practices throughout the project and help ensure that SECURE-NET outputs remain accessible, trustworthy, and valuable beyond the project's lifetime.

References

[1] SECURE-NET Grant Agreement, Project 101217315, 2025, https://cordis.europa.eu/project/id/101217315

[2] EU Data management plan document https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/temp-form/report/data-management-plan_he_en.docx

[3] The European Code of Conduct for Research Integrity REVISED EDITION 2023 https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/european-code-of-conduct-for-research-integrity_horizon_en.pdf