D1.2

Data Management Plan

Project number:	101070627
Project acronym:	**REWIRE**
Project title:	Rewiring the Compositional Security Verification and Assurance of Systems of Systems Lifecycle
Project Start Date:	1st October, 2022
Duration:	36 months
Programme:	HORIZON-CL3-2021-CS-01
Deliverable Type:	Report
Reference Number:	HORIZON-CL3-2021-CS-01-101070627/ D1.2 / v1.0
Work package:	WP 1
Due Date:	31/03/2023
Actual Submission Date:	31/03/2023
Responsible Organisation:	UBITECH
Editor:	Dr. Stylianos Kazazis
Dissemination Level:	PU
Revision:	v1.0
Abstract:	This report provides an analysis of the data management policy that will be used by the applications regarding all the artefacts that will be generated in the context of REWIRE project.
Keywords:	Data Management Plan, FAIR data, Open Research Data Pilot

The project REWIRE has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101070627

Versioning and contribution history

Version	Date	Author	Notes
0.1	17/01/2023	Dr. Stylianos Kazazis, Thomas Krousarlis, Christina Stratigaki (UBITECH)	ToC, Request for partners input
0.2	20/02/2023	Dr. Stylianos Kazazis, Eleni-Nora Papatsoutsou (UBITECH)	Updates on Chapter 2
0.3	01/03/2023	All partners	Updates on Chapter 3
0.4	03/03/2023	Dr. Stylianos Kazazis, Eleni-Nora Papatsoutsou (UBITECH)	Updates on Chapter 4
0.5	06/03/2023	Dr. Stylianos Kazazis, Eleni-Nora Papatsoutsou (UBITECH)	Updates on Chapter 5
0.6	08/03/2023	Dr. Stylianos Kazazis, Eleni-Nora Papatsoutsou (UBITECH)	Updates on Chapter 6
0.7	09/03/2023	Dr. Stylianos Kazazis, Eleni-Nora Papatsoutsou (UBITECH)	Final version, ready for internal review
0.8	10/03/2023	Dr. Stylianos Kazazis, Eleni-Nora Papatsoutsou (UBITECH)	Release for internal review
0.9	30/03/2023	Spiros Koussouris (SUITE5), Ena Kurtovic (SECURA)	Internal Review, Addressing reviewers' comments
1.0	31/03/2023	Dr. Stylianos Kazazis (UBITECH)	QA review and submission

Disclaimer

The information in this document is provided "as is", and no guarantee or warranty is given that the information is fit for any particular purpose. The content of this document reflects only the author's view – the European Commission is not responsible for any use that may be made of the information it contains. The users use the information at their sole risk and liability. This document has gone through the consortium's internal review process and is still subject to the review of the European Commission. Updates to the content may be made at a later stage.

Executive Summary

Following European Commission's Guidelines for Horizon Europe to submit a Data Management Plan (DMP) as a deliverable within the first six (6) months of the project, this report provides an analysis of the data management policy that will be used by the applications regarding all the research datasets that will be generated by the REWIRE project. Any occurring further updates in this respect will be provided during the project lifespan, on the basis of the actual developments of the technical work. More specifically, in line with the F.A.I.R Principles, this deliverable presents how making the research data collected and/or generated throughout and after the project duration Findable, Accessible, Interoperable and Re-usable. The DMP is, thus, a key document presenting the data management practices employed by consortium partners, describing -among other- standards and methodology for data collection and generation will be followed, and whether and how data will be shared. To this end, partners were requested to provide input with respect to the artefacts that they all will produce/provide in the REWIRE project and the level of dissemination (Public/Sensitive).

The present DMP should be maintained as a living document and updated over the course of the project, whenever significant changes arise either with respect to the data management practices of individual partners or at project level. Note that a detailed description of the data management practices concerning -in particular- processing of personal data in the context of webinars, surveys and questionnaires will be provided under WP1, D1.3 Legal and Ethical issues and Guidelines deliverable, due to M24 of REWIRE project.

Contents

List of Figures

List of Tables

Chapter 1
Introduction

1.1 Scope and Purpose

This deliverable presents the REWIRE data management plan, as captured in M6 of the project. In accordance with European Commission's Guidelines for Horizon Europe (HE) Programme [1], to submit a Data Management Plan (DMP) within the first six (6) months of the project, the present report forms the DMP of REWIRE project reflecting the technical progress at the moment of the drafting of the present document. Further updates in this respect will be provided in the course of the project duration, on the basis of the actual developments of the technical work. More specifically, in line with the F.A.I.R Principles, the deliverable provides for how making the research data collected and/or generated throughout and after the project duration Findable, Accessible, Interoperable and Re-usable. To this end, the deliverable outlines -among other- how the research data collected and/or generated will be handled during and after the REWIRE project, describes which standards and methodology for data collection and generation will be followed, and whether and how data will be shared. Note that the document is largely based on the related template provided by the European Commission (EC) [2].

This DMP outlines how data collected or generated by the REWIRE project will be organised, stored, and shared. It specifies the types of research data that will be generated or collected during the project, the standards that will be used, how the research data will be preserved and what parts of the datasets will be shared for verification or reuse.

The present report forms a deliverable -primarily- addressed to:

- European Commission
- Partners and Advisory Group in the REWIRE project
- EU Parliament
- Horizon Europe projects and other cyber/digital security related projects (clustering activities)
- Organizations and experts involved in the REWIRE case studies.
- Other relevant organizations both public and private, including associations of relevant stakeholders

1.2 Relation to other WPs and Deliverables

The delivery of the present document falls under Work Package (WP) 1 activities and specifically Task 1.2, which extends until M36 of REWIRE project. In the context of the related activities, it is, thus, intended that the DMP is a living document, subject to updates -to the extent necessary- on the basis of the progress of the project activities. It should be noted that a detailed description of the data management practices concerning -in particular- processing of personal data in the context of webinars, surveys and questionnaires will be provided under WP1, D1.3 Legal and Ethical issues and Guidelines deliverable, due to M24 of REWIRE project. Also, DMP, is strongly related with all WPs of REWIRE project since it supports the data management life cycle for all research data that will be collected, processed, or generated within the project.

Chapter 2
Data Management in Horizon Europe

According to the EC, DMPs are a cornerstone for responsible management of research outputs, notably data and are mandatory in Horizon Europe for projects generating and/or reusing data [3].

The DMP is defined as:

“A Data Management Plan (DMP) is a document that outlines from the start of the project the main aspects of the lifecycle of research outputs, notably including data. This includes their provenance, organisation and curation, as well as adequate provisions for their access, preservation, sharing, and eventual deletion, both during and after a project. Writing a DMP is an activity directly linked to the methodology of the research, i.e. good data management will make the work more efficient/save time, contribute to safeguarding information and to increasing the impact and the value of the data among the beneficiaries and others, during and after the research.”

The purpose of a DMP is to provide a discussion of the main elements of the data management policy that will be used by the applicants with regard to all the datasets that will be generated by the project.

Overall, having taken into account all relevant principles regarding lawful processing of personal data, scientific research data should be easily discoverable, accessible, assessable and intelligible, useable beyond the original purpose for which it was collected and interoperable to specific quality standards.

The REWIRE Data Management also follows the Horizon Europe Data Management Plan Template, released by the European Commission Directorate – General for Research & Innovation [2]. This Horizon DMP template has been designed to be applicable to any Horizon Europe project that produces, collects or processes research data. According to these guidelines the management and organization of data should be based on four basic principles, which determine how research outputs should be processed so that they can be more easily accessed, understood, exchanged and reused. This means that data must be findable, accessible, interoperable and re-useable, for example by researchers interested in using the data in further research in the field.

These principles precede implementation choices and do not necessarily suggest any specific technology, standard, or implementation-solution. EC provides a Template with the FAIR principle. This template is not intended as a strict technical implementation of the FAIR principles, it is rather inspired by FAIR as a general

concept. The template represents the set of questions that someone should answer with a level of detail appropriate to the project.

Table 2.1: Clarification of terms

Type	Responsible
Research data	Research data is the evidence that underpins all research conclusions (except those which are purely theoretical) and includes data that have been collected, observed, generated, created or obtained from commercial, government or other sources, for subsequent analysis and synthesis to produce original research results. These results are then used to produce research papers and submitted for publication.
Open research data	Openly accessible research data can typically be accessed, mined, exploited, reproduced and disseminated, free of charge for the user
Secondary data	Secondary data are data that already exist, regardless of the research to be conducted
Open access	Open access is understood as the principle that research data should be accessible to relevant users, on equal terms, and at the lowest possible cost. Access should be easy, user-friendly and, if possible, Internet-based.
Metadata	Metadata is data used to describe other data. It summarizes basic information about data, which can make finding and working with instances of data easier.
Research data repositories	Research data repositories are online archives for research data. They can be subject based/thematic, institutional or centralized.

It is possible to develop a single DMP for any project to cover overall approach. However, where there are specific issues for individual datasets (e.g. regarding openness), someone should clearly spell this out.

The template proposes the following issues to be addressed:

- Data Summary
- FAIR data
- Allocation of resources
- Data security
- Ethical aspects
- Other issues
- Further support in developing your DMP

Each of the previously defined has its own set of questions that has to be addressed. The proposed template states that it is not required to provide detailed answers to all the questions of the DMP that needs to be submitted by month 6 of the project, subject -also- to potential future updates. Rather, the

DMP is intended to be a living document -to the extent necessary- in which information can be made available on a finer level of granularity through updates as the implementation of the project progresses and when significant changes occur.

Chapter 3
REWIRE Data Management Overview

As described in the Guidelines on FAIR Data Management in Horizon Europe a Data Management Plan is a key element to ensure data is well managed. For this reason, in this section we will firstly identify the type of artefacts that will be generated and collected in the framework of the project. During the lifetime of the REWIRE project, several artefacts will be produced. The artefacts that will be collected/generated are listed below in Section 3.2. As the project evolves, this list may require modifications (addition or removal of artefacts) with respect to the project developments.

3.1 Types and Formats of Artefacts Generated/Collected

In order to provide an overview of the different data sets that are currently and will be produced in the REWIRE project, the following table shows the data type, the related WP number and the format, in which the data will be presumably stored.

Table 3.1: Artefacts overview

#	Artefact type	Explanation	WP#	Format (indicative)
1	Research Item	Models and Meta models, Policies, Questionnaires, Deliverables, Papers	2-7	.xls, .csv, .txt, .docx, .pdf
2	Software	Code, APIs, microservices, libraries, dashboard	2-5	.xls, .csv, .txt, .docx, .pdf
3	Dataset	Synthetic, dummy	2-6	.xls, .csv, .txt, .docx, .pdf

3.2 REWIRE Artefacts and Access

In the survey contacted during the first months of the project, the input collected from most of the partners is depicted in the following chart. The types of REWIRE Artefacts are distributed as 13% being datasets, 49% research items and the remaining 38% is of a software artefact type.

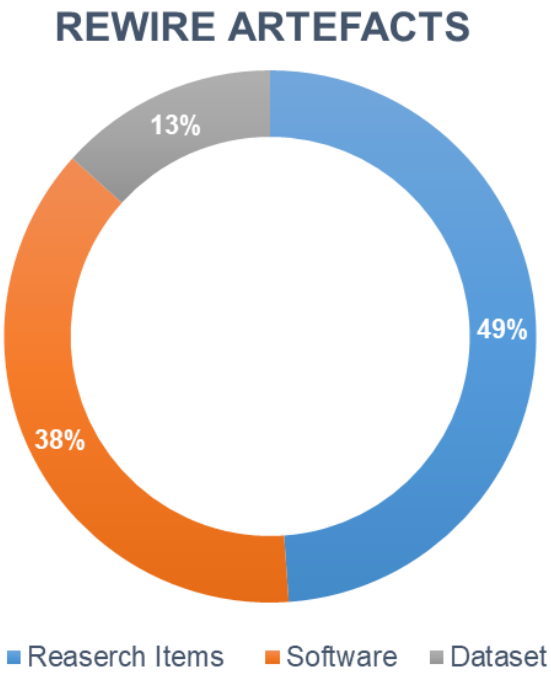

Figure 3.1: REWIRE artefacts' types

3.2.1 Research Items

The following table present the current status and consensus within the Consortium with regards to the current identified research items and their access rights. It is provisioned that this table is a recurring exercise and all future updates and additions will be documented under the relevant deliverables. Note that the information below, provided by partners, is currently available at the project's repository (here) and is monitored regularly.

Table 3.2: Partners' Research Item provision

Partner	Artefact Description	Publishable (P)/Non-Publishable (N-P)
UBITECH	Deliverable D2.1	P
UBITECH	Deliverable D4.3	P
UBITECH	Scientific publications	P
UCL	Deliverable D2.2	P
UCL	Deliverable D3.2	P
UCL	Scientific publications	P
SECURA	Deliverable D3.3	P
NEC	Deliverable 4.1	P
NEC	Deliverable 7.3	N-P

TUD	Deliverable 5.1	P
TUD	Scientific publications	P
SUITE5	Deliverable 4.2	P
UNIS	Deliverable 6.1	N-P
8BELLS	Deliverable 7.1	P
ODINS	Scientific publications	P
ODINS	Deliverable D6.2	N-P
UTRCI	Deliverable D3.1	P
UTRCI	Scientific publications	P
SURREY	Deliverable D5.2	P
SURREY	Deliverable D7.2	P
SURREY	Scientific publications	P
SURREY	Cryptographic protocols	P

3.2.2 Software

The following tables present the current status and consensus within the Consortium with regards to the current identified artefacts of software type provided in the context of REWIRE project, along with relevant information accompanying them (Artefact description, Dataset description, Format/Type, End user, Existence of similar data, Possibility of integration and reuse, Standards and metadata, Data sharing, Archiving and preservation). As stated previously, it is provisioned that the tables presented in this subsection are recurring exercises and all future updates and additions will be documented under the relevant deliverables. Note that the information below, provided by partners, is currently available at the project's repository (here) and is monitored regularly.

3.2.2.1 Trust assessment framework

Owner	UBITECH
Artefact Description	Definition of a trust architecture capturing the trust model and trust relationships of the next generation Systems of Systems. The framework is composed of of two related elements: i) an automated, real-time risk assessment mechanism that will enable an IoT device to calculate the required trust level needed to cooperatively execute a certain function addressing the identified risks, ii) a reasoning mechanism to infer the actual trust level that can be placed into a remotely executed function or externally received data
Dataset description	Library of data harmonization and trust management techniques for extracting (during runtime) the types of security claims that need to be produced by devices as

	measures of evidence on their trustworthiness
Format/Type	Code
End user	Users of the REWIRE platform
Existence of similar data	Partially for other types of hardware devices
Possibility of integration and reuse	The framework will be developed to be as generic as possible to be easily adaptable to other devices.
Standards and Metadata	The code will be documented through inline source code comments, and/or reference manuals. The documentation of the code may be done with standardised tools such as Doxygen.
Data Sharing	To be agreed
Archiving and preservation	Partner private repository

3.2.2.2 Runtime tracer

Owner	UBITECH
Artefact Description	Tracing mechanisms that will be used for extracting the control- and data-flow graphs. This provides the trusted anchor with the compiled control- and information-flow graphs that represent the runtime state of a remote device, against the configuration and execution properties of safety-critical components to be verified
Dataset description	Algorithms to identify On-board unit system traces efficiently and correctly, towards providing runtime properties that can be used as indicators on the level of trust of the target device. This can include configuration integrity tracing and control-flow tracing of IoT device functions running as part of the provided service landscape
Format/Type	Code
End user	The tracing extensions will be made available to the scientific community
Existence of similar data	The goal is to target purely software-based runtime tracing capabilities, thus, existing libraries may be investigated in this direction including the “extended Berkeley Filters” execution hooks and tracing functionalities.
Possibility of integration and reuse	These tracing extensions may be used to support the monitoring and introspection of devices that are also outside the ones to be leveraged in the REWIRE use cases.
Standards and Metadata	Source-code of proof-of-concept implementations will be developed and will be disseminated as open-source.
Data Sharing	The tracing algorithms and primitives will be disseminated through scientific publications.
Archiving and preservation	Partner private repository

3.2.2.3 Risk assessment engine

Owner	UBITECH

Artefact Description	For the risk evaluation, a meta-model will be defined that will include assets such as deployed devices (comprising the mixed-criticality services of the target supply chain) and datasets with their properties and their relationships and dependencies. Security and privacy calculation will be related to the ISO and GDPR definitions, respectively, and will also take into account the possible risks that are related with the device configuration and execution behavioural properties so as to identify the best set of mitigation strategies (i.e., security attestation policies) to be enforced
Dataset description	A reactive run-time Risk Assessment and mitigation framework will be developed to ensure the security of the envisioned use cases in the face of emerging threats and vulnerabilities. This RA tool will take informed decisions on updating and patching critical software and firmware resources, and identify risks from deviations of the behaviour profile of devices
Format/Type	Code
End user	The risk assessment and vulnerability analysis will be made available to users of the REWIRE platform
Existence of similar data	Partially for other types of hardware devices
Possibility of integration and reuse	The framework will be developed to be as generic as possible to be easily adaptable to other devices
Standards and Metadata	The code will be documented through inline source code comments, and/or reference manuals. The documentation of the code may be done with standardised tools such as Doxygen
Data Sharing	It hasn't yet been agreed up to what extent and under which licence the code will be made available. However, the outputs of the risk assessment models to the envisioned use cases will be kept confidential
Archiving and preservation	The outputs of the risk assessment tool will be preserved for 3-30 years at the partner's private repositories

3.2.2.4 REWIRE Trust Execution Environment (TEE)

Owner	NEC
Artefact Description	REWIRE TEE as a trusted reference model for Risc-V processors based on Keystone
Dataset description	N/A
Format/Type	Code
End user	The risk assessment and vulnerability analysis will be made available to users of the REWIRE platform
Existence of similar data	Keystone TEE
Possibility of integration and reuse	Should be deployed/reused on any compatible platform
Standards and Metadata	The code will be documented through inline source code comments, and/or reference manuals. The documentation of the code may be done with standardised tools such as Doxygen
Data Sharing	It hasn't yet been agreed up to what extent and under which licence the code will be made available.

Archiving and preservation	The outputs of the risk assessment tool will be preserved for 3-30 years at the partner's private repositories

3.2.2.5 Secured modes of operation

Owner	UCL
Artefact Description	Symmetric cipher mode of operation
Dataset description	N/A
Format/Type	Code
End user	Users of the REWIRE platform
Existence of similar data	N/A
Possibility of integration and reuse	Should be deployed/reused on any compatible platform
Standards and Metadata	The code will be documented through inline source code comments, and/or reference manuals. The documentation of the code may be done with standardised tools such as Doxygen
Data Sharing	It hasn't yet been agreed up to what extent and under which licence the code will be made available. Probably, it will be available under open-source licence
Archiving and preservation	Partner's private repository

3.2.2.6 Automotive Use Case business logic software in target devices

Owner	KENOTOM
Artefact Description	Demo functionalities reproducing common automotive applications will be developed for the Automotive Use Case.
Dataset description	N/A
Format/Type	Code
End user	Users of the REWIRE platform
Existence of similar data	Depending on the selected target device, sample applications may be available.
Possibility of integration and reuse	Should be deployed/reused on any compatible platform
Standards and Metadata	The code will be documented through inline source code comments, and/or reference manuals. The documentation of the code may be done with standardised tools such as Doxygen
Data Sharing	It hasn't yet been agreed up to what extent and under which licence the code will be made available.

Archiving and preservation	Partner's private repository

3.2.2.7 Blockchain and Smart Contract Protocols

Owner	TUD
Artefact Description	The REWIRE blockchain and smart contracts infrastructure, which is used to support management lifecycle and threat intelligence data sharing to improve cybersecurity awareness in heterogeneous IoT deployments.
Dataset description	N/A
Format/Type	Code
End user	Users of the REWIRE platform
Existence of similar data	N/A
Possibility of integration and reuse	Should be deployed/reused on any compatible platform
Standards and Metadata	The code will be documented through inline source code comments, and/or reference manuals. The documentation of the code may be done with standardised tools such as Doxygen
Data Sharing	It hasn't yet been agreed up to what extent and under which licence the code will be made available. Probably, it will be available under open-source licence
Archiving and preservation	Partner's private repository

3.2.2.8 Secure oracles

Owner	TUD
Artefact Description	The REWIRE Secure decentralized oracles for the interaction of smart contracts with the off-chain (external) data sources.
Dataset description	N/A
Format/Type	Code
End user	Users of the REWIRE platform
Existence of similar data	N/A
Possibility of integration and reuse	Should be deployed/reused on any compatible platform
Standards and Metadata	The code will be documented through inline source code comments, and/or reference manuals. The documentation of the code may be done with standardised tools such as Doxygen

Data Sharing	It hasn't yet been agreed up to what extent and under which licence the code will be made available. Probably, will be available under open-source licence
Archiving and preservation	Partner's private repository

3.2.2.9 Attestation agent

Owner	SURREY
Artefact Description	Implementation of attestation schemes including Instruction Set Architecture execution flow from the design phase
Dataset description	N/A
Format/Type	Code
End user	The risk assessment engine
Existence of similar data	N/A
Possibility of integration and reuse	Should be deployed/reused on any compatible platform
Standards and Metadata	The code will be documented through inline source code comments, and/or reference manuals. The documentation of the code may be done with standardised tools such as Doxygen
Data Sharing	It hasn't yet been agreed up to what extent and under which licence the code will be made available. Probably, will be available under open-source licence
Archiving and preservation	Partner's private repository

3.2.2.10 TEE wallet

Owner	SURREY
Artefact Description	Used to store keys and other confidential data. The basic component of the key management system.
Dataset description	N/A
Format/Type	Code
End user	Users of the REWIRE platform
Existence of similar data	N/A
Possibility of integration and reuse	Should be deployed/reused on any compatible platform
Standards and Metadata	The code will be documented through inline source code comments, and/or reference manuals. The documentation of the code may be done with standardised tools such as Doxygen

Data Sharing	It hasn't yet been agreed up to what extent and under which licence the code will be made available. Probably, will be available under open-source licence
Archiving and preservation	Partner's private repository

3.2.2.11 Security policy enforcer

Owner	SURREY
Artefact Description	Uses evidence from the attestation agent to control the issuance of the verifiable credentials used to access the system and provide input to the risk assessments.
Dataset description	N/A
Format/Type	Code
End user	Users of the REWIRE platform
Existence of similar data	N/A
Possibility of integration and reuse	Should be deployed/reused on any compatible platform
Standards and Metadata	The code will be documented through inline source code comments, and/or reference manuals. The documentation of the code may be done with standardised tools such as Doxygen
Data Sharing	It hasn't yet been agreed up to what extent and under which licence the code will be made available. Probably, it will be available under open-source licence
Archiving and preservation	Partner's private repository

3.2.2.12 Smart Cities Use Case business logic software in target devices

Owner	ODINS
Artefact Description	Demo functionalities reproducing common Smart Cities applications will be developed for the Smart Cities Use Case.
Dataset description	N/A
Format/Type	Code
End user	Users of the REWIRE platform
Existence of similar data	Depending on the selected target device, sample applications may be available.
Possibility of integration and reuse	Should be deployed/reused on any compatible platform
Standards and Metadata	The code will be documented through inline source code comments, and/or reference manuals. The documentation of the code may be done with standardised tools such as Doxygen

Data Sharing	It hasn't yet been agreed up to what extent and under which licence the code will be made available.
Archiving and preservation	Partner's private repository

3.2.2.13 "Flatsat" testbed software source code

Owner	LSF
Artefact Description	Source code of all subsystem software of the indicative "Flatsat" used as a testbed for the Smart Satellites use case, including basic developers documentation.
Dataset description	N/A
Format/Type	Code
End user	Users of the REWIRE platform
Existence of similar data	Artefact shall be based on available open source components
Possibility of integration and reuse	Modular design to maximize reuse
Standards and Metadata	The code will be documented through inline source code comments, and/or reference manuals. The documentation of the code may be done with standardised tools such as Doxygen and Sphinx
Data Sharing	Open Source, preferably GPLv3, to the extent toolchains allows it
Archiving and preservation	Partner's public GitLab repository

3.2.2.14 "Flatsat" testbed hardware source code

Owner	LSF
Artefact Description	Source code of all subsystem hardware of the indicative "Flatsat" used as a testbed for the Smart Satellites use case, including basic developers documentation.
Dataset description	N/A
Format/Type	Code
End user	Users of the REWIRE platform
Existence of similar data	Artefact shall be based on available open source components
Possibility of integration and reuse	Modular design to maximize reuse
Standards and Metadata	The code will be documented through inline source code comments, and/or reference manuals. The documentation of the code may be done with standardised tools such as Sphinx

Data Sharing	Open Source, preferably CERNv2-OHL-S
Archiving and preservation	Partner's public GitLab repository

3.2.2.15 Binary analysis engine

Owner	SECURA
Artefact Description	Semi-automatic binary analysis, using static and dynamic methods to discover vulnerabilities in firmware and software
Dataset description	N/A
Format/Type	Code
End user	Users of the REWIRE platform
Existence of similar data	Similar (semi-)automatic binary analysis platforms
Possibility of integration and reuse	Is already reused in a similar EU project, SANCUS.
Standards and Metadata	The code will be documented through inline source code comments, and/or reference manuals. The documentation of the code may be done with standardised tools such as Doxygen
Data Sharing	It hasn't yet been agreed up to what extent and under which licence the code will be made available. Probably, it will be available under open-source licence
Archiving and preservation	Partner's public repository

3.2.2.16 AI-based Misbehaviour Detection

Owner	SUITE5
Artefact Description	The component will perform AI-based misbehaviour detection using the data (or pointers) collected on the blockchain (or on the off-chain storage)
Dataset description	N/A
Format/Type	Code
End user	Users of the REWIRE platform
Existence of similar data	N/A
Possibility of integration and reuse	Should be deployed/reused on any compatible platform
Standards and Metadata	The code will be documented through inline source code comments, and/or reference manuals. The documentation of the code may be done with standardised tools such as Doxygen

Data Sharing	It hasn't yet been agreed up to what extent and under which licence the code will be made available
Archiving and preservation	Partner's public repository

3.2.2.17 Formal Verification processes of hardware designs

Owner	UTRCI
Artefact Description	A tool chain that will be used to formally verify and validate the secure and trusted operation of crypto mechanisms and security protocols in order to ensure that they will serve robustly during runtime to support the safety-critical operation of IoT deployments
Dataset description	A semi-automated VHDL generation framework will be able to automatically synthesize the end-hardware description that will realize the custom system-on-chip for the specified requirements.
Format/Type	Code
End user	Users of the REWIRE platform
Existence of similar data	N/A
Possibility of integration and reuse	Should be deployed/reused on any compatible platform
Standards and Metadata	The code will be documented through inline source code comments, and/or reference manuals. The documentation of the code may be done with standardised tools such as Doxygen
Data Sharing	It hasn't yet been agreed up to what extent and under which licence the code will be made available
Archiving and preservation	Partner's public repository

3.2.3 Dataset

The following tables present the current status and consensus within the Consortium with regards to the current identified artefacts of dataset type provided in the context of REWIRE project, along with relevant information accompanying them (Dataset description, Format/Type, End user, Existence of similar data, Possibility of integration and reuse, Standards and metadata, Data sharing, Archiving and preservation). As stated previously, it is provisioned that the tables presented in this subsection are recurring exercises and all future updates and additions will be documented under the relevant deliverables. Note that the information below, provided by partners, is currently available at the project's repository (here) and is

monitored regularly.

3.2.3.1 Experimental measurements

Owner	UNIS, WP6 contributors
Dataset Description	The performance of demonstrators will be evaluated by measurements aiming to assess the operation and benefits of the REWIRE in the context of the respective application domains towards enhancing the operational and functional safety of the IoT deployments. Those might include timing and power consumption or recordings of measurement data that will be provided depicting ECU's or IoT MCU's information, diagnostic functionalities, and relevant REWIRE performance metrics (e.g., time of completion of software update)
Format/Type	.csv
End user	Experimental results may be included in scientific publications and utilised for the evaluation of the REWIRE platform
Existence of similar data	Performance metrics are typically included in scientific publications wherein attestation and/or cryptography is addressed
Possibility of integration and reuse	The results may be used in other publications for performance comparisons
Standards and Metadata	Experimental results will be published under the form of an Excel or a CSV file
Data Sharing	Publicly available through Zenodo or Gitlab
Archiving and preservation	The experimental results will be preserved for 3-30 years at the partners' private and public repositories

3.2.3.1 Threat intelligence for misbehaviour detection training dataset

Owner	SUITE5
Dataset Description	Runtime tracer logs to train AI algorithms (existing software and firmware vulnerabilities)
Format/Type	.csv, json
End user	Experimental results may be included in scientific publications
Existence of similar data	N/A
Possibility of integration and reuse	The results may be used in other publications for performance comparisons
Standards and Metadata	Experimental results will be published under the form of an Excel as a CSV file or JSON
Data Sharing	Publicly available through Zenodo or Gitlab
Archiving and preservation	The experimental results will be preserved for 3-30 years at the partners' private and public repositories

3.2.3.2 Runtime tracer data logs

Owner	UBITECH
Dataset Description	Datasets generated based on execution flows of systems consisting of sequences of Assembly instructions
Format/Type	.csv
End user	Experimental results may be included in scientific publications
Existence of similar data	N/A
Possibility of integration and reuse	The results may be used in other publications for performance comparisons
Standards and Metadata	Experimental results will be published under the form of an Excel or a CSV file
Data Sharing	Publicly available through Zenodo or Gitlab
Archiving and preservation	The experimental results will be preserved for 3-30 years at the partners' private and public repositories

3.2.3.3 (System) requirements, use cases (system) architecture

Owner	UBITECH
Dataset Description	These documents describe the requirements of the REWIRE framework and the use-case system architecture and will establish concrete goals for the remainder of the project
Format/Type	.docx
End user	The REWIRE documentation will be made available to the public so that other groups may contribute to the project or take advantage of it
Existence of similar data	N/A
Possibility of integration and reuse	The system requirements and architecture may be used as a basis for other projects on security, privacy and operational assurance services in various application domains
Standards and Metadata	Experimental results will be published under the form of a Word file.
Data Sharing	The documentation will be made publicly available through Zenodo or Gitlab
Archiving and preservation	The experimental results will be preserved for 3-30 years at the partners' private and public repositories

3.3 Expected size of the data (if known)

It is expected that as a research outcome will generate research datasets (i.e. results of the technologies, services of the demos, etc.), publications, new services proposal, dissemination material, etc. Due to size

of the project, scope of work and complexity, the expected size cannot be estimated at the moment.

Chapter 4
REWIRE ORDP Participation

The Open Research Data Pilot (ORDP) of the European Commission enables open access and reuse of research data generated by Horizon Europe projects. There are two main pillars to the Pilot: a) developing a DMP and b) providing open access to research data.

A project that opts-in ORDP have to adhere to the following conditions:

- Develop (and keep up-to-date) DMP.
- Deposit the data in a research data repository.
- Ensure third parties can freely access, mine, exploit, reproduce and disseminate this data.
- Provide related information and identify (or provide) the tools needed to use the raw data to validate the research.

The ORDP applies to:

- The data (and metadata) needed to validate results in scientific publications.
- Other curated and/or raw data (and metadata) that are specified in the DMP.

From the current consensus within the consortium some of the REWIRE Artefacts will not be publicly available as depicted in the graphics below (Figure 4.1, Figure 4.2 and Figure 4.3).

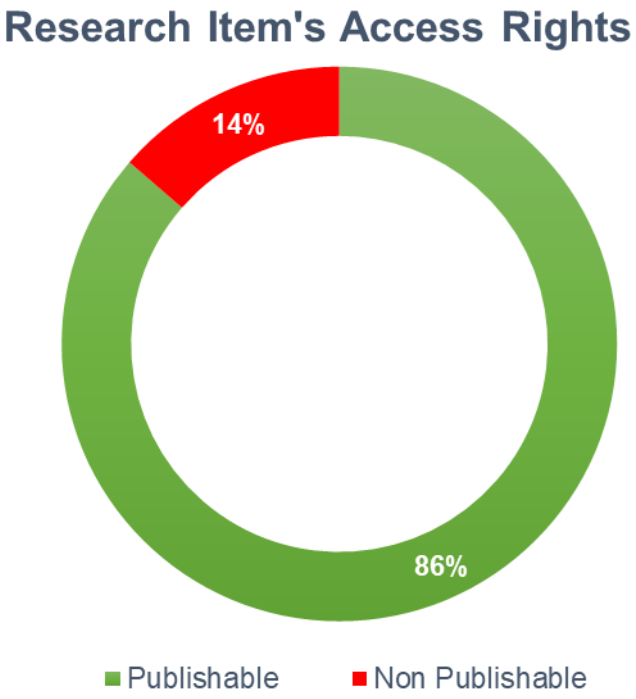

Figure 4.1: Research items artefacts access rights

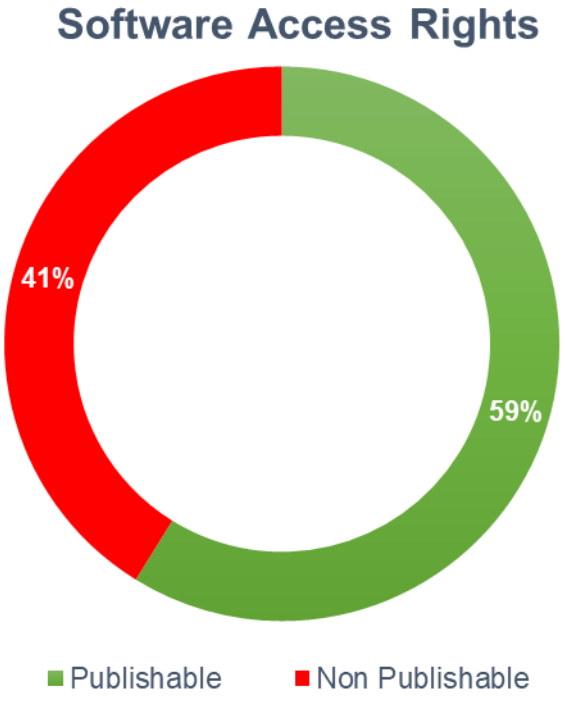

Figure 4.2: Software artefacts access rights

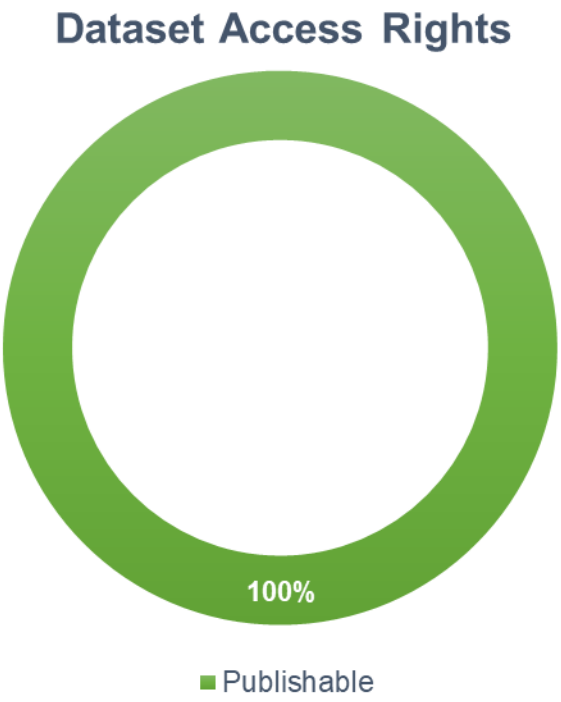

Figure 4.3: Dataset artefacts access rights

4.1 Publishing Infrastructure for Open Access

The REWIRE publication infrastructure consists of a process and several web-based publication platforms that together provide long-term open access to all publishable, generated or collected results of the project. The implementation of the project will be done in accordance with the applicable regulations in national and EU level and, especially, with the General Data Protection Regulation (GDPR) protection of personal data [4].

More specifically, there are not cases where personal data information or sensitive information of internet users is collected (IP addresses, email addresses or other personal information) or further processed. In the potential future case where the REWIRE consortium will collect and/or further process personal data, this will be done in accordance with GPDR. Overall, it is aimed that REWIRE only collects and/or further processes personal data are necessary for the attainment of the project objectives. Both the process and the used web-based platforms are described in the following subsections.

4.1.1 Publishing Process

REWIRE partners defined a simple, deterministic process that decides if a result in REWIRE must be published or not. The term result is used for all kind of artefacts generated during REWIRE like white papers, scientific publications, and anonymous usage data. By following this process, each result is either classified public or non-public. Public means that the result must be published under the open access policy. Non-public means that it must not be published. For each result generated or collected during

REWIRE runtime, the following questions must be answered to classify it:

Does a result provide significant value to others or is it necessary to understand a scientific conclusion?
If this question is answered with yes, then the result is classified as public. If this question is answered with no, the result is classified as non-public. Such a result could be code that is very specific to REWIRE platform (e.g., a database initialization) which is usually of no scientific interest to anyone, nor does it add any significant contribution.
Does a result include personal information that is not the author's name?
If this question is answered with yes, the result is classified as non-public. Personal information beyond the name must be removed if it should be published. This also bears witness on the repetitive nature of the publishing process, where results which are deemed in the beginning as non-publishable can become publishable once privacy-related information is removed from them.
Does a result allow the identification of individuals even without the name?
If this question is answered with yes, the result is classified as non-public. Sometimes data inference can be used to superimpose different user data and reveal indirectly a single user's identity. As such, in order to make a result publishable, the included information must be reduced to a level where single individuals cannot be identified. This can be performed by using established anonymization techniques to conceal a single user's identity, e.g., abstraction, dummy users, or non-intersecting features.
Does a result include business or trade secrets of one or more partners of REWIRE?
If this question is answered with yes, the result is classified as non-public, except if the opposite is explicitly stated by the involved partners. Business or trade secrets need to be removed in accordance to all partners' requirements before it can be published.
Does a result name technology that is part of an ongoing, project-related patent application?
If this question is answered with yes, then the result is classified as non-public. Of course, results can be published after patent has been filed.

Can a result be abused for a purpose that is undesired by society in general or contradict with societal norms and REWIRE's ethics?
If this question is answered with yes, the result is classified as non-public.
Does a result break national security interests for any project partner?
If this question is answered with yes, the result is classified as non-public.

4.1.2 Publishing Platforms

In REWIRE, we use several platforms to publish our results openly. The following list presents the platforms used during the project and describes their concepts for publishing, storage, and backup.

The project Website

The partners in the project consortium decided early to setup a project-related website. This website describes the mission and the general approach of REWIRE and its development status. A blog informs about news on a regular basis. Later in the project the developed REWIRE platform will be announced. A dedicated area for downloads is used to publish reports and white papers as well as scientific publications (in pre-camera ready form, or through links to the publisher's websites in case these are not open access). All documents are published using the portable document format (PDF)[1]. All downloads are enriched by using simple metadata information, such as the title and the type of the document. The website is hosted by partner UBITECH whereas is moderated and regularly updated by partner 8BELLS. All webpage-related data is backed up on a regular basis. All information on the project website can be accessed without creating an account. The website is backed up once per month.

Zenodo

Zenodo is a research data archive / online repository which helps researchers to share research results in a wide variety of formats for all fields of science. It was created through EC's OpenAIRE+ project and is now hosted at CERN using one of Europe's most reliably hardware infrastructures. Data is backed nightly and replicated to different locations. Zenodo not only supports the publication of scientific papers or white papers, but also the publication of any structured research data (e.g., using XML). Zenodo provides a connector to GitLab that supports open collaboration for source code and versioning for all kinds of data. All uploaded results are structured by using metadata, like for example the contributors' names, keywords, date, location, kind of document, license, and others. Considering the language of textual metadata items, English is preferred. All metadata is licensed under CC0 license (Creative

[1] Note that the site will not host spreadsheets. It exclusively host PDFs

Commons 'No Rights Reserved'). The property rights or ownership of a result does not change by uploading it to Zenodo. All public results generated or collected during the project lifetime will be uploaded to the dedicated Zenodo community created (here) for long-term storage and open access.

GitLab

GitLab is a well-established online repository which supports distributed source code development, management, and revision control. It is primarily used for source code data. It enables world-wide collaboration between developers and provides also some facilities to work on documentation and to track issues. GitLab provides paid and free service plans. Free service plans can have any number of public, open-access repositories with unlimited collaborators. Private, non-public repositories require a paid service plan. Many open-source projects use GitLab to share their results for free. The platform uses metadata like contributors' nicknames, keywords, time, and data file types to structure the projects and their results. The terms of service state that no intellectual property rights are claimed by GitLab over provided material. For textual metadata items, English is preferred. All source-code components that are implemented during this project and decided to be public will be uploaded to an open access GitLab repository (here).

4.1.3 Access and Sharing

The accessing and sharing of data is firstly ruled by two documents: the non-disclosure agreement, which stipulates under which conditions transmitted information between the project partners is deemed confidential and must not be further disseminated; and the Description of Action (DoA) which stipulates the dissemination level of each deliverable. Moreover, the project consortium will comply with the FAIR (findable, accessible, interoperable and reusable) (European Commission, 2016) guidelines of the Horizon Europe programme.

The data necessary to successfully complete the project WPs will be shared without any restrictions amongst the WP partners either via internal repositories or direct communication. Public data will be made available at the project's website or other repositories, as appropriate. Users will be made aware of this data primarily through research publications, patent applications, dissemination activities, invited talks, social networks and the project website. Data will be made available to the project consortium as soon as it is available; to standardization bodies when required; and to the public at the due date of the derivable, and, in case a research publication is based on that, as soon as the paper is submitted (if submission is anonymous, this will be postponed). If access to confidential data is necessary by the public, restrictive measures will be put in place.

Chapter 5
FAIR Data

REWIRE project supports the reuse of research data and follows FAIR principles [5]. FAIR represents a set of guiding principles to make data Findable, Accessible, Interoperable, and Reusable. The international FAIR Principles have been formulated as a set of guidelines for the reuse of research data. The acronym FAIR stands for findable, accessible, interoperable and reusable. Research data must be of quality that makes them accessible, findable and reusable.

Findable: data has a unique, persistent ID, located in a searchable resource, and documented with meaningful metadata.

Accessible: data is readily and freely retrievable using common methods and protocols, metadata is accessible even if the data is not.

Interoperable: data is presented in broadly recognized standard formats, vocabularies, and languages.

Re-useable: data has clear licenses, and accurate meaningful metadata conformity to relevant community standards and identifying its content and provenance.

5.1 Making Data Findable, Including Provisions for Metadata

This document launches the data management plan to support the effective collection and integration of the REWIRE data. Storage, processing and sharing (among project participants) will occur via data exchange platforms (such as Microsoft Sharepoint), whereas interaction with the wider public will be achieved through the official project website. Also, data will be stored at the coordinator's repository and will be kept for minimum 5 years after the end of the project. Where requested, data will be kept for 2 more years.

A naming convention will include a concise description of contents, the host institution collecting the data and the month of publication.

Version numbering will only be an issue if a participant requests withdrawal of their data in which case a version number will be added to the filename.

No specific standards or metadata have been identified for the time being for the proposed datasets.

Data will be anonymized meaning that data will not identify any individuals and therefore real names of participants will NOT be distributed.

Data will be shared only in relation to publications (deliverables and papers). As such, the publication will serve as the main piece of metadata for the shared data. When this is not seen as being adequate for the comprehension of the raw data, a report will be shared along with the data explaining their meaning and methods of acquisition.

5.1.1 Discoverability of the data

In order to be able to use the data generated by the project it is essential to integrate data from the participants in the open calls and the activities undertaken by project partners. Taking into account the FAIR data principles [6] (meta)data should:

- Be assigned to a globally unique and persistent identifier;
- contain enough metadata to fully interpret the data, and;
- Be indexed in a searchable source.

By applying these principles data become retrievable and include their authentication and authorization details.

5.1.2 Data identification mechanisms

All documents associated project will be identified with a project name and unique and persistent document type designator and number that will be given to the coordinator for the submission to the EC. Versioning of the document should be part of the document name and title.

As per the documents related to project activities and/or deliverables, the tasks or deliverables number will be used to identify the document followed by a brief title of the activity or deliverable.

Example

REWIRE- D1.2 - Data Management Plan -v1.0.pdf

5.1.3 Naming conventions used

Each set of data produced (dataset, deliverables, etc.) will be named in a uniform way and will include a table with a version control.

The recommendations to name documents of the project are as follows [7]:

- Choose easily readable identifier names (short and meaningful)

- Do not use acronyms that are not widely accepted
- Do not use abbreviations or contractions
- Avoid Language-specific or non-alphanumeric characters
- Add a two-digit numeric suffix to identify new versions of one document
- Dates should be included back to front and include the four-digit years: YYYYMMDD.

For deliverables: **REWIRE_[Deliverable Code]-[Deliverable Title]_[Partner]-vA.BB** i.e.: REWIRE_D1.1-Project Handbook-v1.00 *(for submission to the Commission)*

For datasets: **WP [Work Package number] P [Pilot number; pilot activity number] - [description of the activity]** i.e.: WP4 P1.3 Results of demonstration performance.

5.1.4 Clear versioning of the documents

Only documents created by the consortium will be versioned, for this purpose templates include 3 descriptors to identify the versions and status of the documents:

Table 5.1: Proposed document history table overview

Version	Date	Author	Notes
1	xx	xx	xx
2			
3			
4			

Moreover, partners, following the recommendations included in section “Naming conventions” will identify the different versions by using a two-digit number following the descriptor Draft. A document reviewed by another partner should be returned to the principal author by including rev + acronym of the organisation. Only the principal author will change the draft number and will add the word FINAL to documents ready to be sent to the EC or those to be used as final versions.

The document history included in the document template should be filled in as follows:

Table 5.2: Document history template - example

Version	Date	Author	Notes
1	XX/XX/2023	ABC	Section 2.1 needs to be completed
2	XX/XX/2023	CDE	Section 2,1 completed. Comments added to the document.
3	XX/XX/2023	ABC	Added suggestions by CDE
4	XX/XX/2023	XYZ	Included some topics on

			section 2.1
	XX/XX/2023	ABC	Final version with partners contribution

5.1.4 Standards for metadata creation (if any)

Basic metadata will be used to facilitate the efficient recall and retrieval of information by project partners and external evaluators and contribute to easily find the information requested. To this end, all documents related to the project have to include in the front-page information about author(s) & editor(s), WP, dissemination level and version.

To support the completeness of metadata, the project provides a metadata template to all stakeholders. The template will be a living document that might be expanded to fit project specific requirements.

Table 5.3: Metadata template for REWIRE datasets.

#	Field	Description
1	Title	A name given to the resource.
2	Creator	An entity primarily responsible for making the resource
3	Subject	The topic of the resource
4	Description	e.g., abstract, table of contents, graphics, ...
5	Publisher	Only for published items.
6	Contributor	Entities that contributed to the making of the resource.
7	Date	The termination of the data collection period.
8	Type	[dataset, article, questionnaire, ...]
9	Format	File format of the resource.
10	Identifier	e.g., ISSN if your item has been published
11	Source	Which tools were used to collect the data
12	Language	A language of the resource.
13	Relation	A related resource.
14	Rights	Information about rights held in and over the resource.

In addition to the dataset's metadata document, dataset providers are compelled to attach additional documents such as:

1. A description of the study
2. Method of research
3. Applied questionnaires
4. Data documentation / usage manual
5. Any other information that might be of interest to a data user

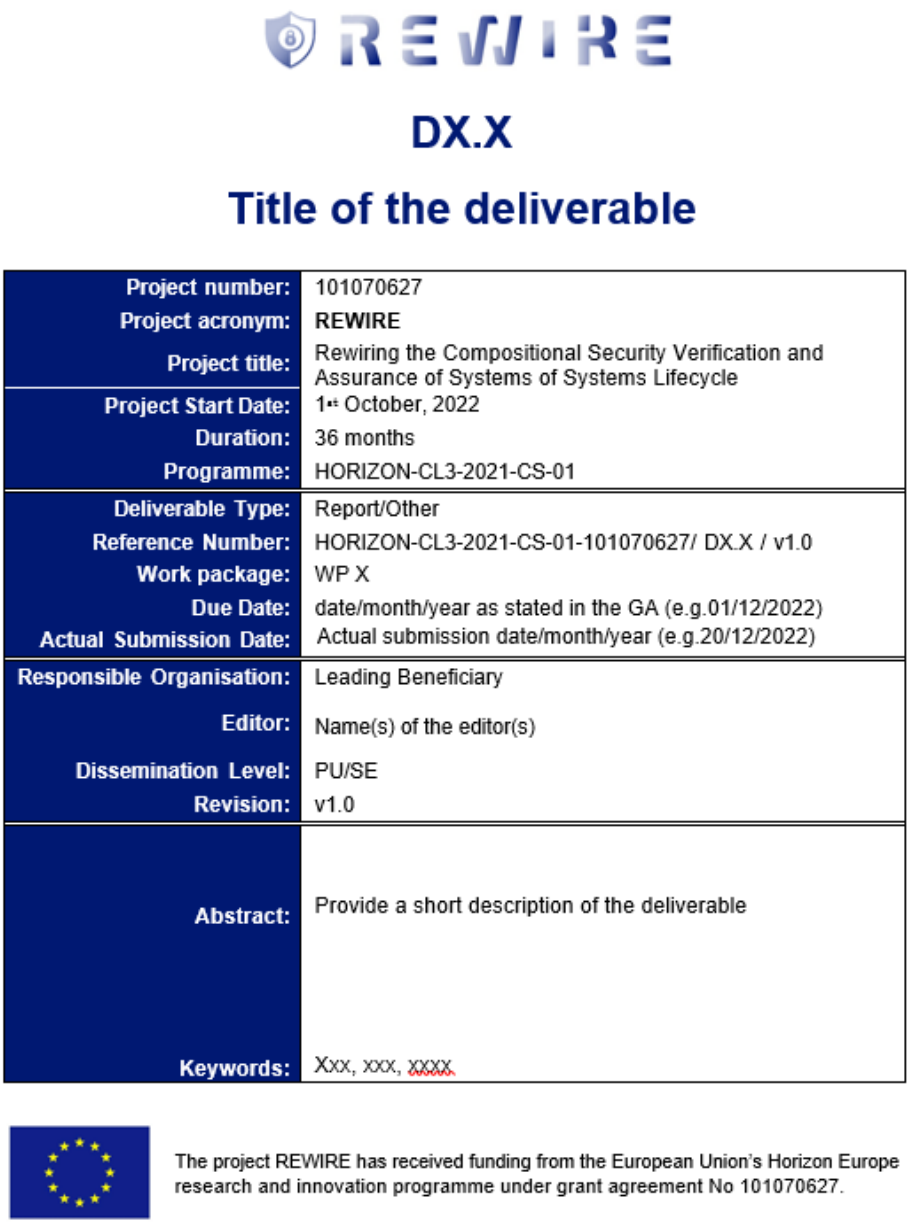

Figure 5.1: Template to be used for project documentation metadata overview

5.2 Making Data Openly Accessible

Where possible data will be made available subject to Ethics and participant agreement. However, the personally-identifiable nature of the data collected within REWIRE means that in most instances it would be difficult to release collected data. Where data is made available, we will do so using the Project's file repository hosted in coordinator's premises.

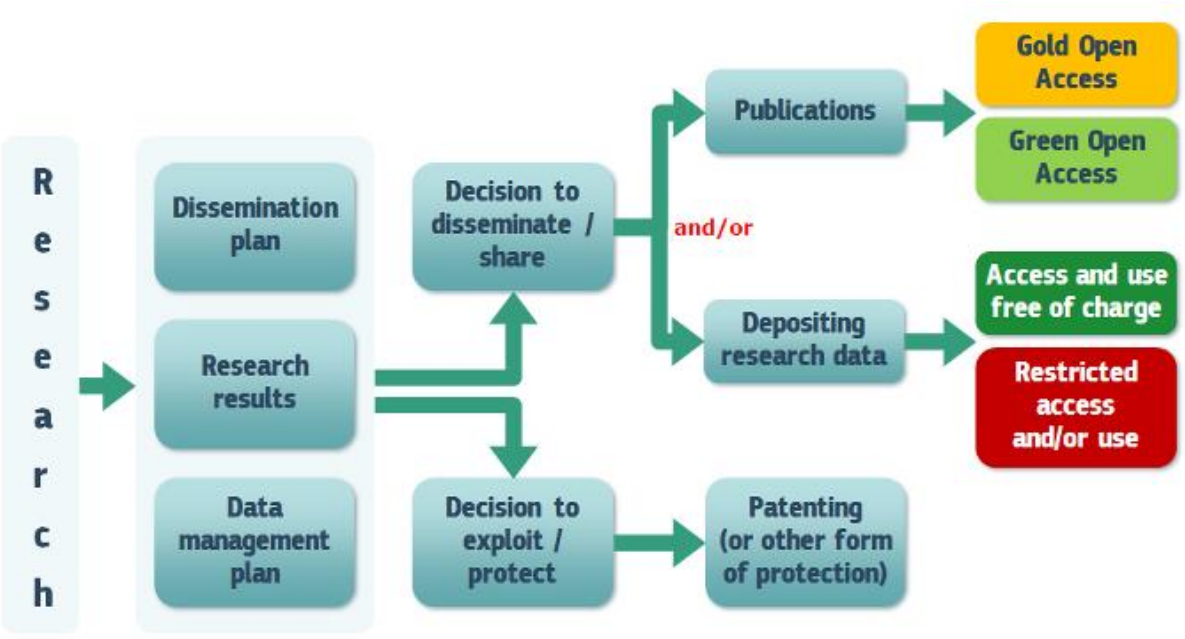

Figure 5.2: Open access to scientific publication and research data in the wider context of dissemination and exploitation [8]

Prior to release, a requesting party will need to contact the Project Coordinator describing their intended use of a dataset. The Project Coordinator will send a terms and conditions document for them to sign and return. Upon return, the dataset will be released. Documentation will be included with the release of the data.

In alignment with the EC Guidelines on Open Access to Scientific Publications and Research Data in Horizon Europe, REWIRE will also follow a combination of Gold and Green Open Access strategy to its scientific publications, which will be agreed during the first months of the project execution. Gold Access will be encouraged for high-impact journal publications while the self-archiving, Green Access will be granted for the rest of the publications. The repositories listed in OpenDOAR, zenodo funded by OpenAIRE and the repositories available through the consortium members will be considered while there will also be a relevant repository on the website of the project and in social networking sites for scientists and researchers like ResearchGate.

5.2.1 Methods or software needed to access the data

No specific software tools will be needed to access the data, since anonymous data sets will be saved and stored in word, pdf or excel to facilitate its exploitation and guarantee their long-term accessibility.

5.2.2 Deposit of data, associated metadata, documentation and code

Data will be deposited and secured on Microsoft Sharepoint file repository and additional instance of all data on coordinator's account.

5.3 Making Data Interoperable

The concept interoperable demands that both data and metadata must be machine-readable and that a consistent terminology is used.

5.3.1 Interoperability of data assessment

Partners will be responsible of storing the data in a comprehensive format and adapted to the real and current needs of the possible practitioners interested in using, merging or exploiting the data generated throughout the project. The assessment of data interoperability will be updated in future reviews in order to guarantee the REWIRE data fits the needs of a specific scenario such as data infrastructures, interests or purpose of data.

5.3.2 Vocabulary use

The vocabulary used in the project is a very standard and common language within the business creation culture and the logistics. Vocabulary won't represent any barrier for data interoperability a re-use.

5.4 Making Data Re-usable

For data to be re-usable, it is -generally- considered that meta(data) have a plurality of accurate and relevant attributes and that they are released with a clear and accessible data usage license. Moreover, it is considered that (meta) data are associated with their provenance and that they meet domain-relevant community standards [9].

Note that the overall management of knowledge and the provisioning for the establishment of the related Intellectual Property Rights is dictated in detail under REWIRE's Grant Agreement and the consortium agreement stipulating -among other- for the ownership of the background and the foreground knowledge, as well as for the commercial exploitation of the project's results.

5.4.1 Increase data re-use through clarifying licenses

Data will only be available on project's Microsoft Sharepoint and their use will be restricted to the research use of the licensee and colleagues on a need-to-know basis. This non-commercial licence is renewable after 2 years, data may not be copied or distributed and must be referenced if used in publications. These arrangements will be formalised in a User Access Management licence which describes in detail the permitted use of the data.

5.4.2 Data quality assurance process

The project coordinator will be responsible of assuring the quality of the data by making sure dataset follow the FAIR principles included in this plan, and that data is updated.

Personal data processing will be done following the EU, national and international laws taking into account the “data quality” principles listed below [10] :

Data processing is adequate, relevant and non-excessive;

- Accurate and kept up to date;
- Processed fairly and lawfully;
- Processed in line with data subjects’ rights;
- Processed in a secure manner;
- Kept for no longer that necessary and for the sole purpose of the project.

Data quality assurance process will be led in accordance with the REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

5.4.3 Length of time for which the data will remain re-usable

The Consortium will contribute to maintain data re-usable as long as possible after the end of the project. A first period of 4 years has been established; however, this time can be extended under partners’ agreement. This period can vary depending on the value of the data after the end of the project.

5.5 Artefact Template

The following tables try to capture the description of the data that will be produced in the context of REWIRE. Every use case will fill in such a template and subsequently all the templates will be collected with the beginning of WP6, the demonstration applications work package of the project.

Table 5.4: Making data findable template

Making data Findable	
Name of data set	*Univocal identifier of the considered data* *[REWIRE _Wx_Tz_01]* *Please, provide one sentence description.*
Data types	*[Real time data stream, unstructured like tweets, synthetic data stream, log data of IDS, etc.]*
Data generation and/or collection	*Description of the type of input used to generate the data and the complete methodology and tools used for data collection*
Purpose	*What are the data collected/generated specifically used for?*
Data origin	*[Where applicable, information from applications to be developed by the partner.]*

Table 5.5: Making data accessible template

Making data Accessible	
Accessibility	*Open/Confidential*
Repository	*Description/location of the available data.*
Shareability restrictions / related Information	*[Where applicable, information from applications to be developed by the partner.]*

Table 5.6: Making data interoperable template

Making data Interoperable	
Format	*Data format, measuring unit, typical order of magnitude [JSON-like, CSV]*
Expected size of the data	*[To be defined, 3 TB/Day or 12 GB/day when compressed etc.]*
Standards and metadata[2]	*[The metadata attributes list. The used methodologies.]*
Standard software Interfaces	*List of the standards used to promote results replicability.*
Extensions to standard interfaces	*Extensions to the above standards as developed during the project.*

Table 5.7: Making data re-usable template

Making data Re-usable	
Re-use of existing data	*[No reuse of existing data, for the generation of synthetic datasets, it will be essential to create a recipe, reusing the existing data in logs etc.]*
Data types	*Consistent location of the data, including previous releases*
Data backup	*Constraints determining the quality/currency of the collected data.*
Quality Consistency	*Description/location of possible emulation tools useful for replicating the data*

[2] Note that the fields pertinent to standards are, also, relevant for reusability purposes.

Chapter 6
Allocation of Resources

6.1 Data management responsibilities

Data will be stored at the Collaboration file repository (Microsoft Sharepoint), set by the Coordinator as the project's repository, and will be kept for 5 years after the end of the project. Where requested, data will be kept for 2 more years. The handling of the repository on behalf of REWIRE as well as all data management issues related to the project fall in the responsibility of the coordinator.

As for the publications, where the analyses of the empirical research data will be presented, the consortium will publish them in scientific journals that allow open access. The costs related to open access will be claimed as part of the Horizon Europe grant.

Regarding the data resulting from the activities of the project, each WP leader will be responsible for the storage and compliance of the data and then for uploading in the REWIRE sharepoint web portal, or other storage systems to share the information of the project.

The REWIRE's coordinator assisted by the WP leaders will be responsible for updating this document and develop a strategy to encourage:

- the identification of the most-suitable data-sharing and preservation methods;
- the efficient use of data assuring clear rules on its accessibility;
- the quality of the data stored and
- the storage in a secured in a user-friendly interface.

6.2 Cost of potential value of long-term preservation

As stated in previous section, the costs of data storage and maintenance are not going to require extra funding once the project ends. As per the value of the data, it is important to take into account that the topics covered by the project respond to a current need of the logistics sector and customers' needs. Therefore, data coming out of this project will have a direct impact in the coming years but might not be of relevance as the challenges are being tackled or replaced by other priorities.

Chapter 7
Data Security

REWIRE data exchange platform (Microsoft Sharepoint) applies technological and organizational measures to secure processing of personal data against publishing to unauthorized persons, processing in violation of the law and change, loss, damage or destruction.

- Information security: Secure Socket Layer certificates are applied. In order to ensure the appropriate level of security, the password for the account will exist on the platform only in a coded encrypted form.
- Options for reading data: the platform offers the possibility to make data available in a read-only or downloadable format, hindering the access to information by unauthorized users.
- Back-up policy: complete and redundant back-ups are done every week. Moreover, every time a modification is done an older version is saved.
- Accidental deletion or modifications: in case of a catastrophic event that implies the partial or complete deletion of the data sets, the data from the most recent back up will be automatically restored (back-up won't be older than 60 minutes). In case of accidental deletion or modification only the most recent document will be restored, so in case of accidental changes or deletion data can be easily recovered.
- Deletion or modification of data by users: only administrators have the rights to delete or modify the information included in the datasets.
- Terms and conditions: the Microsoft Sharepoint platform have specific terms of use and conditions that have to be accepted by all users of the platform.

Chapter 8
Ethics Aspects

The REWIRE consortium is aware of the ethical aspects pertinent to the scope of REWIRE, which are addressed under the WP 1, Task 1.3 on “Legal and ethics monitoring”.

This task defines how research will be executed in the project regarding the ethics issues during the implementation of the REWIRE (including, but not limited to, confidentiality, integrity, validity, objectivity, accuracy, transparency, trustworthiness, authenticity, respect for autonomy, reciprocity and equity), in collaboration with the project partners and the independent ethics committee that will be established and operate during the project implementation to closely monitor and consult the consortium with regards to any activity involving ethics issues.

List of Abbreviations

Abbreviation	Translation
DMP	Data Management Plan
HE	Horizon Europe
WP	Work Package
EC	European Commission
EU	European Union
TEE	Trust Execution Environment
VHDL	Very High-speed integrated circuit hardware Description Language
IoT	Internet of Things
DoA	Description of Action
ECU	Electronic Control Unit
MCU	Micro-Controller unit

References

[1] EU Grants: AGA – Annotated Grant Agreement, art 17, V0.2 DRAFT - 30.11.2021, available at: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/common/guidance/aga_en.pdf

[2] A template for a DMP is provided under the reporting templates in the reference documents of the Funding and Tenders portal of the European Commission, available at: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/how-to-participate/reference-documents;programCode=HORIZON

[3] EU Grants: HE Programme Guide, art 16, V2.0 - 11.04.2022, available at: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/programme-guide_horizon_en.pdf

[4] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[5] Force11 (2016) The FAIR Data Principles, https://www.force11.org/group/fairgroup/fairprinciples

[6] Wilkinson, M. D. et al. The FAIR Guiding Principles for scientific data management and stewardship. Sci. Data3:160018 doi: 10.1038/sdata.2016.18 (2016).

[7] https://www.ukdataservice.ac.uk/manage-data/format/organising

[8] European Commission Directorate-General for Research & Innovation (2017) Guidelines on Open Access to Scientific Publications and Research Data in Horizon 2020

[9] See, also, FAIR data principles (FORCE11 discussion forum) available at: https://www.force11.org/group/fairgroup/fairprinciples

[10] Wilms, G. Guide on Good Data Protection Practice in Research of the European University Institute. (March 2017). Retrieved from http://www.eui.eu/Documents/ServicesAdmin/DeanOfStudies/ResearchEthics/Guide-Data-Protection-Research.pdf