Ref. Ares(2023)2360193 - 31/03/2023

Scaling Up secure Processing, Anonymization and generation of Health Data for EU cross border collaborative research and Innovation

SECURED

EU Project

D1.1 — Project Handbook Quality, Risk Management

Funded by
the European Union

Grant Agreement Nr. 10109571

Project Information

Project Title	Scaling Up Secure Processing, Anonymization and Generation of Health Data for EU Cross Border Collaborative Research and Innovation		
Project Acronym	SECURED	**Project No.**	10109571
Start Date	01 January 2023	**Project Duration**	36 months
Project Website	https://secured-project.eu/		

Project Partners

Num.	Partner Name	Short Name	Country
1 (C)	Universiteit van Amsterdam	UvA	NL
2	Erasmus Universitair Medisch Centrum Rotterdam	EMC	NL
3	Budapesti Muszaki Es Gazdasagtudomanyi Egyetem	BME	HU
4	ATOS Spain SA	ATOS	ES
5	NXP Semiconductors Belgium NV	NXP	BE
6	THALES SIX GTS France SAS	THALES	FR
7	Barcelona Supercomputing Center Centro Nacional De Supercomputacion	BSC CNS	ES
8	Fundacion Para La Investigacion Biomedica Hospital Infantil Universitario Nino Jesus	HNJ	ES
9	Katholieke Universiteit Leuven	KUL	BE
10	Erevnitiko Panepistimiako Institouto Systimaton Epikoinonion Kai Ypolgiston-emp	ICCS	EL
11	Athina-Erevnitiko Kentro Kainotomias Stis Technologies Tis Pliroforias, Ton Epikoinonion Kai Tis Gnosis	ISI	EL
12	University College Cork - National University of Ireland, Cork	UCC	IE
13	Università Degli Studi di Sassari	UNISS	IT
14	Semmelweis Egyetem	SEM	HU
15	Fundacio Institut De Recerca Contra La Leucemia Josep Carreras	JCLRI	ES
16	Catalink Limited	CTL	CY
17	Circular Economy Foundation	CEF	BE

Project Coordinator: Francesco Regazzoni - University of Amsterdam - Amsterdam, The Netherlands

Copyright

© Copyright by the SECURED consortium, 2023.

This document may contains material that is copyright of SECURED consortium members and the European Commission, and may not be reproduced or copied without permission. All SECURED consortium partners have agreed to the full publication of this document.

The technology disclosed herein may be protected by one or more patents, copyrights, trademarks and/or trade secrets owned by or licensed to SECURED partners. The partners reserve all rights with respect to such technology and related materials. The commercial use of any information contained in this document may require a license from the proprietor of that information. Any use of the protected technology and related material beyond the terms of the License without the prior written consent of SECURED is prohibited.

Disclaimer

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

Except as otherwise expressly provided, the information in this document is provided by SECURED members "as is" without warranty of any kind, expressed, implied or statutory, including but not limited to any implied warranties of merchantability, fitness for a particular purpose and no infringement of third party's rights.

SECURED shall not be liable for any direct, indirect, incidental, special or consequential damages of any kind or nature whatsoever (including, without limitation, any damages arising from loss of use or lost business, revenue, profits, data or goodwill) arising in connection with any infringement claims by third parties or the specification, whether in an action in contract, tort, strict liability, negligence, or any other theory, even if advised of the possibility of such damages.

Deliverable Information

Workpackage	WP1
Workpakace Leader	Francesco Regazzoni (UvA)
Deliverable No.	D1.1
Deliverable Title	Project Handbook Quality, Risk Management
Lead Beneficiary	UvA
Type of Deliverable	Report
Dissemination Level	Public
Due Date	31/03/2023

Document Information

Delivery Date	23/03/2023
No. pages	29
Version | Status	2.0 | Final
Deliverable Leader	Francesco Regazzoni (UvA)
Internal Reviewer #1	Konstantinos Avgerinakis (CTL)
Internal Reviewer #2	Luca Pulina (UNISS)

Quality Control

Approved by Internal Reviewer #1	30/03/2023
Approved by Internal Reviewer #2	31/03/2023
Approved by Workpackage Leader	31/03/2023
Approved by Quality Manager	31/03/2023
Approved by Project Coordinator	31/03/2023

List of Authors

Name(s)	Partner
Francesco Regazzoni, Maureen Voestermans, Angelica da Silva Lantyer	UvA
Paolo Palmieri	UCC

The list of authors reflects the major contributors to the activity described in the document. The list of authors does not imply any claim of ownership on the Intellectual Properties described in this document. The authors and the publishers make no expressed or implied warranty of any kind and assume no responsibilities for errors or omissions. No liability is assumed for incidental or consequential damages in connection with or arising out of the use of the information contained in this document.

Revision History

Date	Ver.	Author(s)	Summary of main changes
22.02.2023	0.1	Maureen Voestermans (UvA), Francesco Regazzoni (UvA)	Created the document and the initial version of its content
06.03.2023	0.2	Francesco Regazzoni (UvA), Paolo Palmieri (UCC)	Adapted to the project template
08.03.2023	0.3	Maureen Voestermans (UvA), Francesco Regazzoni (UvA)	Added the risk management section
09.03.2023	0.3	Angelica da Silva Lantyer (UvA), Francesco Regazzoni (UvA)	Added management structure figure
10.03.2023	1.0	Francesco Regazzoni (UvA)	Version ready for internal review
31.03.2023	2.0	Francesco Regazzoni (UvA)	Included internal reviewers requests and comments from other partners

Table of Contents

1 Executive Summary 8
1.1 Related Documents 8

2 Introduction 9
2.1 Structure of the Document 9

3 Project Management Structure 10
3.1 Project Roles 10
3.1.1 Project Coordinator 10
3.1.2 Project Manager 11
3.1.3 Project Controller 11
3.1.4 Work Package Leaders 11
3.1.5 Exploitation Leader 11
3.1.6 Dissemination Leader 12
3.1.7 Data Protection Leader 12
3.1.8 Quality Manager 12
3.1.9 Appointments 12
3.1.10 Taks Leaders 12
3.1.11 Deliverable Leaders 13
3.2 Project Committees 13
3.2.1 General Assembly 13
3.2.2 Executive Board 13
3.3 Project Coordination Team 14
3.4 Project Meetings 14
3.4.1 Consortium meetings 14
3.4.2 General Assembly meetings 15
3.4.3 Executive Board Meetings 15

4 Document Management 16
4.1 Document Templates 16
4.2 Documents Naming Conventions 16
4.3 Documents exchange 17

5 Document Quality Assurance 18

6 Resource Management 21
6.1 Internal Progress Reports 21
6.2 Responsibility Assignment 21

7 Communication 22

8 Publications, Public Presentations, and Dissemination 24

9 Risk Management and Conflict Resolution Procedures 25

10 Conclusions 28

A Project Logo 29

Acronyms and Abbreviations

CA	Consortium Agreement. 8, 9
DoA	Description of Actions. 8, 9, 21
GA	Grant Agreement. 8, 9, 14, 21, 22
PC	Project Coordinator. 10–13
WP	Work Pakage. 22, 25

1 Executive Summary

This deliverable, D1.1 Project Handbook Quality, Risk Management, describes the SECURED management and quality assessment procedures. It addresses issues related to project structure, organization, and control, partner responsibilities and describes the internal procedures, the communication mechanisms and the risk assessment and mitigation strategies.

In details, this deliverable presents:

- The management procedures, the key roles, the governing bodies, and the meetings of the project
- The document management, the naming convention and the templates
- The quality assurance procedures
- The means of communication between partners
- The procedure for publications and the required acknowledgements
- The risk management and conflict resolution procedures

This deliverable will serve as a manual and reference document for the project partners to explain the project procedures and to ensure a fruitful and smooth collaboration towards the achievement of the technical, societal and scientific project objectives.

1.1 Related Documents

- Grant Agreement (GA) Project 101095717 - SECURED; Description of Action (DoA) Annex 1
- SECURED Consortium Agreement (CA)

2 Introduction

This document contains the management procedures and guidelines for the SECURED project.

Specifically it addresses:

- Administrative processes and resource management procedures that ensure accurate financial reporting and justification of the work being carried out in the project.
- General project management processes that ensure harmonious and timely coordination of research, technology and development activities that result in high quality deliverables and high quality R&D output, including technical articles and hardware or software prototypes.
- An internal communication strategy that ensures clear and effective communication between Partners and allows for the timely resolution of management and technical issues.
- External communication, dissemination and exploitation processes that ensure a unified presentation of the project to the public.

It is required to read it for all project participants, especially for new personnel. This document is a companion to the Grant Agreement Project 101095717 - SECURED and the SECURED Consortium Agreement. The project handbook may in some instances provide more details in relation to the procedures and processes followed by the consortium but the handbook is strictly subordinate to the legally binding agreements mentioned above. Where there are any inconsistencies between these documents, the following order of precedence should be applied:

- Grant Agreement (GA) Project 101095717 - SECURED; Description of Action (DoA) Annex 1
- SECURED Consortium Agreement (CA)
- Project Handbook Quality, Risk Management (this document)

Any issues related to precedence will be resolved by the Project General Assembly (see Section 3.2.1) as required. This body has the power to amend this handbook as it sees fit throughout the execution of the project. In addition to the contractual version, due in at M3, updates will be made whenever necessary. The Project Coordinator is responsible for its maintenance and updating. This handbook will be downloadable by the public from the SECURED website and by project partners from the SECURED shared folder. Information concerning updates will be duly sent to all partners.

2.1 Structure of the Document

The next section summarizes main SECURED administrative players and Project Management procedures. Section 3 describes the management structures of the project. Section 4 defines procedures for documents creation, sharing, update and management. Section 5 describes the procedure for quality assurance of deliverable. Section 6 describes resource management approach. Section 7 provides means for effective communication. Section 8 defines rules for publications and dissemination of the project results. Finally, Section 9 provides risk management and conflict resolution procedures. The Appendix reports the logo of the SECURED project.

3 Project Management Structure

Project Management, meetings organizations, conflict resolution and risk management are performed according to Grant Agreement Project 101095717 - SECURED and SECURED Consortium Agreements. The overview of SECURED Project Management structure is provided in Figure 1. The overall management structure of the SECURED project is simple and agile, and the roles and the responsibility within that are clearly defined. The goal of the Project Management structure is to efficiently coordinate the activities of the consortium, to ensure the achievement of the project objectives and to guarantee an high quality of the delivered results. Additionally, the Project Management structure should also guarantee the compliance with applicable ethical and data regulation, maximize the international visibility of the project and foster the exploitation of the project outcome.

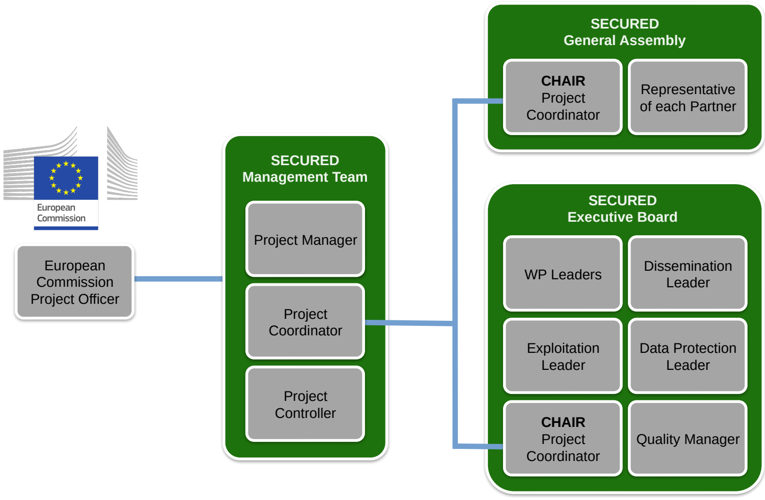

Figure 1 – SECURED Management Structure

3.1 Project Roles

3.1.1 Project Coordinator

The Project Coordinator (PC) is Francesco Regazzoni (UvA), who is also responsible of the technical coordination of the project. In addition to its responsibilities as a Party, the Project Coordinator takes responsibility for the overall management and execution of the project in particular in relation to:

- Rights and obligations as set out in the Grant Agreement
- Rights and obligations as set out in Consortium Agreement
- Successful management of the project in terms of achieving deliverables, reporting, data management, dissemination, administration, financial management and audit
- Communication between the consortium and the European Commission
- Technical coordination: overseeing accomplishment of the scientific and technical objectives and promoting the project's visibility internationally

The Project Coordinator shall not be entitled to act or to make legally binding declarations on behalf of any other Party or of the Consortium. The PC shall have no other functions unless otherwise agreed upon by the General Assembly.

3.1.2 Project Manager

The Project Manager is Angelica da Silva Lantyer (UvA). The Project Managers has the role to assist the PC in ensuring that the project work plan, milestones, and time scales are maintained according to the specifications of the Description of Actions. Tasks of the Project Manager include:

- To assist the PC in the communications with the European Commission
- To assist in the preparation and submission to the European Commission of all deliverables, project reviews and reports
- To help the PC in monitoring the execution progresses of the Project
- To assist the PC in all the administrative aspects of the Project

3.1.3 Project Controller

The Project Controller is Laura Davoli (UvA). The Project Controller is responsible for administering the financial contributions of the European Commission and distributing these to the partners.

3.1.4 Work Package Leaders

The Work Package Leaders (listed in Table 4) are responsible for the completion of their work packages and successful production of deliverables. Work Package Leaders are technical leaders appointed by the partner responsible for each work package. They are responsible for the organization and control of each work package. They direct all aspects of activity in the work package and report to the Executive Board in co-ordination with the Project Coordinator. In detail, the Work Package Leaders responsibilities are:

- To coordinate, monitor and manage the activities under their responsibility, and to ensure the timely achievement of the objectives and milestones of the work packages.
- To prepare the internal and external reports (deliverables) expected for the work package, and assist in the production of the overall management reports of the project.
- To arrange regular technical meetings or conference calls of the work package members. To ensure the accurate recording of times, costs and resources, and report any discrepancies immediately to the Project and Technical Coordinators.
- To organize technical presentations of the work package activities, and to ensure proper involvement and visibility of the active members.
- To inform the Executive Board about progress of activities and possible critical issues.
- To identify the need for creation of separate tasks in the work package.
- To ensure the horizontal flow of information to other work package leaders.
- To identify and report any technical or managerial problems that arise in their work package.

3.1.5 Exploitation Leader

The Exploitation Leader will coordinate the SECURED exploitation and innovation activities, by monitoring the outcomes of the technical process and matching them to business opportunities. The Exploitation Leader will be responsible for linking with industry beyond the consortium. Finally, in cooperation with Dissemination Leader, the Exploitation Leader shall define the optimal communication and dissemination strategies and channels to maximize the impact of the Action.

Work Package	Partner	Name
WP1	UvA	Francesco Regazzoni
WP2	BSC CNS	Alberto Gutiérrez Torre
WP3	SEM	Peter Pollner
WP4	CTL	Christos Avgerinos
WP5	EMC	Christos Strydis

Table 4 – Work Package Leaders

3.1.6 Dissemination Leader

The Dissemination Leader will coordinate the SECURED dissemination and communication activities. The Exploitation Leader will be in charge of defining and updating the dissemination policy and will oversee the production and the maintenance of the Project Website and of all the dissemination material, and will manage the social medias of the project.

3.1.7 Data Protection Leader

The Data Protection Leader will be responsible for overseeing the data protection strategy and implementation to ensure compliance with GDPR requirements and other applicable regulations. The Data Protection Leader will also assist the Project Coordinator in ensuring that the project execution is carried out in compliance with ethical principles (including the highest standards of research integrity) and applicable EU, international and national law, including the EU Charter of Fundamental Rights and the European Convention for the Protection of Human Rights and Fundamental Freedoms and its Supplementary Protocols.

3.1.8 Quality Manager

The Quality Manager will support the Project Coordinator in overseeing the assurance of quality across the project activities, with particular focus on project deliverables and project review(s). A mechanism for the review of project deliverables is defined in Section 5. The Quality Manager will assist the PC in ensuring that goals set by Grant Agreement are fully implemented on a day-to-day basis.

3.1.9 Appointments

The General Assembly appointed Konstantinos Avgerinakis (CTL), Apostolos Fournaris (ISI), Daniela Spajic (KUL), and Paolo Palmieri (UCC) as Exploitation Leader, Dissemination Leader, Data Protection Leader, and Quality Manager, respectively.

3.1.10 Taks Leaders

Each task of a work package is led by one partner. Task Leaders are technical leaders appointed by the partner responsible for each task. Task Leaders report to the corresponding Work Package Leader, co-ordinates the technical work for their activity according to the project and work package objectives, and assists in the preparation of reports. Participants to each task have to be identified and responsibilities have to be clearly defined.

Partner	Name
UVA	Francesco Regazzoni
EMC	Christos Strydis
BME	Gergely Acs
ATOS	Juan Carlos Perez Baun
NXP	Joppe Bos
THALES	Stephane Lorin
BSC CNS	Alberto Gutiérrez Torre
HNJ	Andrés Castillo
KUL	Daniela Spajic
ICCS	Nikolaos Bakalos
ISI	Apostolos Fournaris
UCC	Paolo Palmieri
UNISS	Luca Pulina
SEM	Peter Pollner
JCLRI	Eduard Porta
CTL	Christos Avgerinos
CEF	Anastasia Vayona

Table 5 – Partner Representative in the General Assembly at the moment of the writing

3.1.11 Deliverable Leaders

Each deliverable has a Deliverable Leader, appointed by the lead beneficiary of the deliverable. The Deliverable Leader reports to the corresponding work package leader and co-ordinates technical work for the deliverable according to the project plan. It is responsibility of the Deliverable Leader to decide the format to be used for the preparation of the deliverable.

3.2 Project Committees

3.2.1 General Assembly

The General Assembly, chaired by the Project Coordinator, includes one representative for each partner. The General Assembly supervises the project development, determines its strategic direction and is in charge of the high-level management of the project, addressing all the administrative, contractual, and financial matters. The General Assembly role, responsibilities, rules, and decision-making procedures are extensively detailed in the Consortium Agreement. Decisions of the General Assembly are binding to all project partners and recorded in approved minutes. The representative of each partner in the General Assembly at the moment of the writing are reported in Section 3.2.1.

3.2.2 Executive Board

The main research and innovation overseeing body of the project will be the Executive Board. The EB has responsibility together with the Project Coordinator for monitoring the overall progress and direction of the project, the resources used and the costs incurred and risk evaluation. The Executive Board is chaired by the PC and will also comprise the work package leaders, the Exploitation Leader, the Dissemination Leader, the Data Pro-

Role	Partner	Name
Project Coordinator	UvA	Francesco Regazzoni
WP2 Leader	BSC CNS	Alberto Gutiérrez Torre
WP3 Leader	SEM	Peter Pollner
WP4 Leader	CTL	Christos Avgerinos
WP5 Leader	EMC	Christos Strydis
Exploitation Leader	CTL	Konstantinos Avgerinakis
Dissemination Leader	ISI	Apostolos Fournaris
Data Protection Leader	KUL	Daniela Spajic
Quality Manager	UCC	Paolo Palmieri

Table 6 – Members of the Executive board at the moment of the writing

tection Leader, and the Quality Manager (or their deputy, previously appointed by email). The members of the Executive Board appointed during the kick off meeting are reported in Section 3.2.2. The Executive Board will convene every month either remotely or in person with the aim to review scientific progress, raise issues and answer questions. The Executive Board will report to the General Assembly. The Executive Board will be responsible for:

- Effective execution of the stated tasks and production of scheduled deliverables
- Achievement of work package objectives and of the overall project goals. A hierarchical project delivery model will be assumed where a work package leader is responsible for the overall delivery of the objectives of a work package, and task leaders are responsible for the delivery of individual tasks assigned to a particular work package.
- Significant deviations from the plan of record will be escalated to the GA for resolution. The EB has no formal decision making authority. It shall seek a consensus among the Parties for all actions taken. Where this is not possible issues will be escalated to the GA for resolution.

3.3 Project Coordination Team

The Project Coordination Team consists of the Project Coordinator, Francesco Regazzoni (UvA), the Project Manager, Angelica da Silva Lantyer (UvA), and the Project Controller, Laura Davoli (UvA). Only the members of the Project Coordination Team shall have direct communication with the Project Officer at the European Commission.

3.4 Project Meetings

3.4.1 Consortium meetings

Face-to-face SECURED consortium meetings will take place every six months (approximately), in order to continuously ensure the interaction among work packages and proper discussions which cannot be guaranteed through a sole teleconference. All people involved in the project are encouraged to participate to the Consortium Meetings. Possibility to connect via teleconference will be offered but it is expected that, except for exceptional and justified reasons, at least one person per partner is physically present to the meeting. Unless differently specified, these meetings include a General Assembly meeting. The detailed scheduling of meetings will always be done in advance to allow maximum participation (possibly, at least two months in advance). Agenda and minutes of each meeting will be saved in the project shared repository.

3.4.2 General Assembly meetings

Unless differently specified, the General Assembly will meet face-to-face during the consortium meetings. Ordinary and extraordinary General Assembly meeting will be organized according to the procedure discussed in the Grant Agreement Project 101095717 - SECURED and in the SECURED Consortium Agreement. Agenda and minutes of each meeting will be saved in the project shared repository.

3.4.3 Executive Board Meetings

The Executive Board will meet every month. Unless differently specified, Executive Board Meetings will take place via teleconference. Agenda and minutes of each meeting will be saved in the project shared repository.

4 Document Management

The infrastructure chosen to hold the documentation produced by the project is *Research Drive*, which is based on a Web server where a private and protected project intranet will host all relevant documents, such as:

- Deliverables
- Resource reports
- Cost Claims
- Meeting Minutes
- Contractual Documentation
- Technical Reports and Papers
- Project templates, logos
- Any other relevant documentation

4.1 Document Templates

All documents shall be formatted in accordance with the templates defined by the Consortium. Templates are provided in the following types of documents:

- Documents, Reports, and Deliverables: MS Word template, Libreoffice Writer template, LaTeX template
- Public and internal presentations: MS Power Point template, Libreoffice Impress template, LaTeX template
- Resource report template: MS Excel template, Libreoffice Calc template

These templates are made available to all partners in the project intranet. The leader of each deliverable decides which template shall be used.

4.2 Documents Naming Conventions

Document naming convention is required to keep track of the project technical and administrative resources, along with the history of revisions. The official deliverable shall be named using the following naming format

SECURED_Dw.d_ShortTitle_ACR_Vx.y_YYYYMMDD.ext

Where:

- w : is the work package number
- d: is the deliverable number
- ShortTitle: explanatory short title of the document without spaces and underscores
- ACR: is the short name of the lead beneficiary (see Table 7)
- x: is the version major number
- y: is the version minor number
- YYYY: is the year

- MM: is the month
- DD: is the day
- ext: is the extension (.doc, .pdf, .ppt, .xls, .exe, .zip)

The Internal documents shall be named using the following naming format:

SECURED_TTTd_ShortTitle_WPw_ACR_Vx.y_YYYYMMDD.ext

Where:

- TTT: is a two or three letter acronym of the following
  - TR - Technical Report
  - RR - Resource Report
  - IPR – Internal Progress Report
  - MAG - Meeting Agenda
  - MM - Meeting Minutes
  - MS - Market Studies
  - SW - Software
  - TCM - Teleconference Meeting Minutes
  - TP - Technical Presentation
  - TPC - Technical/Research Publication (Conference)
  - TPJ - Technical/Research Publication (Journal/Magazine)
- d: is the document number given by Project or Scientific Coordinator
- ShortTitle: is an explanatory short title of the document
- w: is the work package number
- ACR: is the partner Acronym that initiated and has the responsibility for the document
- x: is the version major number
- y: is the version minor number
- YYYY: is the year
- MM: is the month
- DD: is the day

Changes in the version number should be applied by the document leader (or, in any case, agreed with the the document leader).

4.3 Documents exchange

The documents exchange server has been provided by the Project Coordinator. After uploading the document, the partner who uploaded the document should inform the relevant consortium members sharing the location of the document or the instructions to reach it.

5 Document Quality Assurance

The official document and emails language will be English. SECURED logo should appear on all SECURED related documents. In case of official deliverables, in addition to document authors, the documents should be reviewed by the two internal reviewers reported in Table 7, by the Work Package Leader, by the Quality Manager and by the Project Coordinator. All the deliverables will be made available to all the partners for further feedback. The timeline for preparing a deliverable is as follows:

1. According to the content of the deliverable, the deliverable leader should commence the process of deliverable preparation in due time, providing a tentative structure of the document as early as possible (unless differently agreed with the workpakage leader, the quality manager, and the project coordinator and duly communicated to all the partners, within two to three months before the deadline). In any case, the final Table of Contents should be circulated by the Deliverable Leader no later than one month before the deadline.
2. The Deliverable Leader, in collaboration with the Work Package Leader, is responsible for collecting all material and formatting the document.
3. The first draft for review should be sent to the internal reviewers, to the Work Package Leader, to the Quality Manager and to the Project Coodinator three weeks before the deadline.
4. The internal reviewers, the Work Package Leader, the Quality Manager and the Project Coordinator will provide detailed feedback two weeks before the deadline.
5. An updated version is prepared by the Deliverable Leader and sent to the Quality Manager and Project Coordinator one week before the deadline, for final approval.

The Document Quality Assurance is depicted in Figure 2.

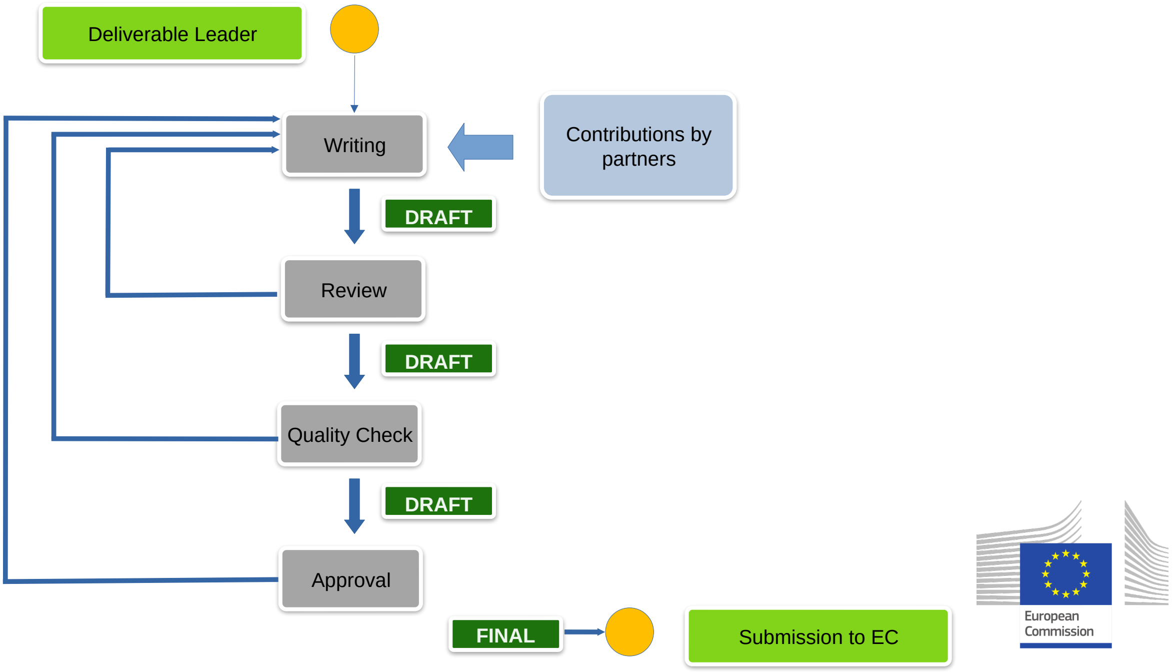

Figure 2 – Quality Assurance Procedure

In case of delay, the Deliverable Leader should suggest a mitigation plan as early as the risk of delay is recognized and coordinate it with the internal reviewers, the Quality Manager and the Project Coordinator. The

Project Coordinator and the Quality Manager may ask additional feedback from other members of the consortium. Before submitting the deliverable, a link to the final version of the deliverable for final approval, along with a final submission date will be sent to all the partners. Any concern should be reported to them before such deadline, otherwise it is considered approved.

No	Name	Due Date	Lead	Reviewer 1	Reviewer 2
D1.1	Project Handbook Quality, Management	31-03-2023	UvA	Konstantinos Avgerinakis, CTL	Luca Pulina, UNISS
D1.7	Project Website	31-03-2023	ISI	Daniela Spajic, KUL	Anastasia Vayona, CEF
D1.2	GDPR and Ethics Project Guidelines	30-06-2023	KUL	Anastasia Vayona, CEF	Gergely Acs, BME
D1.6	Data Management Plan	30-06-2023	UvA	Stephane Lorin, THALES	Nikolaos Bakalos ICCS
D1.9	Dissemination and Exploitation Plan	30-06-2023	ISI	Juan Carlos Pérez Baun, ATOS	Alberto Gutiérrez Torre, BSC
D4.1	State of the Art and initial technical requirements	30-06-2023	ISI	Christos Strydis, EMC	Joppe Bos, NXP
D2.5	Legal and ethical framework and analysis	30-09-2023	KUL	Apostolos Fournaris, ISI	Anastasia Vayona, CEF
D2.1	Interim report on data anonymization, de-anonymization and Synthetic data generation techniques, tools and services	29-02-2024	UCC	Joppe Bos, NXP	Gergely Acs, BME
D3.1	Interim report on Scalable Secure Multiparty Computation, Federated Learning and Unbiased AI techniques and tools	29-02-2024	SEM	Apostolos Fournaris, ISI	Christos Strydis, EMC
D1.4	Market Analysis, IPR Management Exploitation and Standardization	30-06-2024	CTL	Eduard Porta, JCLRI	Juan Carlos Pérez Baun, ATOS
D4.2	Architecture Specifications, Analysis and Design	30-06-2024	ISI	Juan Carlos Pérez Baun, ATOS	Alberto Gutiérrez Torre, BSC
D5.1	Use case requirements and evaluation metrics	30-06-2024	EMC	Konstantinos Avgerinakis, CTL	Luca Pulina UNISS
D1.8	Updated Data Management Plan	31-07-2024	UvA	Nikolaos Bakalos ICCS	Stephane Lorin, THALES
D2.2	Data anonymization and de-anonymization techniques and tools	31-12-2024	ATOS	Péter Polner, SEM	Apostolos Fournaris, ISI
D3.2	Scalability Enhancement for Secure Multiparty Computation	31-12-2024	NXP	Christos Strydis, EMC	Stephane Lorin, THALES
D3.3	Secure Multiparty Computation Federated Learning Client Infrastructure	31-12-2024	BME	Nikolaos Bakalos ICCS	Alberto Gutiérrez Torre, BSC

No	Name	Due Date	Lead	Reviewer 1	Reviewer 2
D5.4	Evaluation and implementation of legal and ethical requirements	31-12-2024	KUL	Luca Pulina UNISS	Eduard Porta, JCLRI
D2.3	Synthetic Data Generation techniques and tools	30-04-2025	BSC	Apostolos Fournaris, ISI	Andrés Castillo, FHUNJ
D2.4	Data anonymization, de-anonymization and Synthetic data generation Library	30-04-2025	UvA	Luca Pulina, UNISS	Christos Strydis, EMC
D3.4	Unbiased AI techniques and methods report	30-04-2025	THAL	Daniela Spajic, KUL	Eduard Porta, JCLRI
D3.5	SECURED Secure Multiparty Computation library, tools and services	30-04-2025	UvA	Stephane Lorin, Thales	Péter Polner, SEM
D4.3	SECURED Solution Formal Verification report	30-04-2025	UNISS	Alberto Gutiérrez Torre, BSC	Joppe Bos, NXP
D4.4	Knowledge Base and SECURED Federation infrastructure	30-04-2025	ICCS	Andrés Castillo, FHUNJ	Daniela Spajic, KUL
D5.2	Use case Development report	30-04-2025	EMC	Konstantinos Avgerinakis, CTL	Gergely Acs, BME
D1.3	Open Call Design, Implementation and Results	30-06-2025	CEF	Daniela Spajic, KUL	Konstantinos Avgerinakis, CTL
D1.5	Updated Market Analysis, IPR Management Exploitation and Standardization	31-12-2025	CTL	Eduard Porta, JCLRI	Juan Carlos Pérez Baun, ATOS
D4.5	SECURED Innohub and Framework Development and Integration	31-12-2025	CTL	Péter Polner, SEM	Andrés Castillo, FHUNJ
D4.6	Legal Validation and Recommendation report	31-12-2025	KUL	Andrés Castillo, FHUNJ	Péter Polner, SEM
D5.3	Use-case Evaluation, Demonstration and Assessment of project results	31-12-2025	EMC	Nikolaos Bakalos ICCS	Joppe Bos, NXP

Table 7 – Reviewers of the Deliverable.

6 Resource Management

For appropriate resource management, resources will be monitored periodically. The reports will be internal and will give a good approximation of the overall resource spending.

6.1 Internal Progress Reports

Before each reporting period or Review Meeting (as such terms are defined or identified in the Grant Agreement (GA) Project 101095717 - SECURED), each partner should submit an internal report (that takes the name of "Internal Progress Report") to the Project Management Team that provides, as further specified below, the progress of each partner in the performance of its tasks and actions in the project. The Internal Progress Report should be submitted within ten (10) working days from explicit request of the Project Coordinator. The Project Coordinator will provide appropriate template including the following issues:

- Major achievements per Partner
- Major difficulties
- Planned resources per work package
- Actual resources per work package
- Cumulative resources per work package
- Conferences/Standardization meetings attended
- Consumables and other expenses

Each Work Package Leader should compile the achievements and difficulties part and provide to the Project Coordinator a section explaining the technical progress in the work package of his/her responsibility.

6.2 Responsibility Assignment

Based on the Grant Agreement Project 101095717 - SECURED; Description of Action (DoA) Annex 1 and the SECURED Consortium Agreement, the Project Coordinator will manage the Work Package Leaders to achieve the objective of each work package. Each Work Package Leader will keep an Action List, detailing the open issues of the work package, the severity of the task, the deadline, and the persons assigned the task, a small description and the issue status (open, assigned, closed, postponed, delayed). The tasks will be assigned to the partners based on their contributions as specified in the Description of Actions, their area of expertise and their resources in the project as reflected by the relevant Person Months.

7 Communication

Ensuring a good communication among project partners and towards outside entities represents an important key of success for the project and a fundamental practice to manage the project at its best. The establishment of a fast, reliable, and easily accessible communications infrastructure is vital to the proper operation of the SECURED project. This can only be achieved through the intensive use of electronic communications (e.g., email, web based exchanges). The project web-site and the social media presence will also be used to enable fast and efficient exchanges of information. The main communication channels for the SECURED project are:

- email,
- telephone/web based conferences, supported where needed by desktop sharing tools,
- bilateral telephone/web based conferences, supported where needed by desktop sharing tools,
- physical meetings.

The *internal communication* includes physical meetings, telephone/web based conferences conferences, exchange of emails, etc. *External communication* includes the dissemination of all project results through publications, project website, social media channels, conferences, events, and the establishment of links to related projects and relevant associations. It will be a responsibility of the Exploitation Leader and of the Dissemination Leader to identify and regularly update the targets of the communication activities.

It is well known that systematic and timely implementation of information flow is central for any Consortium based project. Nevertheless, overflow of information should obviously also be avoided. The communication flow between SECURED members will be implemented by:

- Periodic project meetings
- Periodic meetings of the EB
- Individual working meetings of members of each WP
- Teleconferences and e-mail interchanges (day to day cooperative working infrastructure)

The members of the Project Coordination Team will be in a day-by-day communication and have the duty to communicate on a systematic and frequent basis even if no problems are identified to assure the smooth flow of SECURED activities. All ordinary messages related to a certain work package will be communicated among all partners involved in that work package. Nevertheless, any special important issues or problems within the frame of a specific work package are going to be forwarded to the all the Work Package Leaders and to the Executive Board members. Of course, this formal and detailed hierarchical communication flow, does not exclude by any means ad-hoc direct communication between any partner participants, whenever this is important for the project success.

Besides a plenary mailing list, there is one mailing list for the GA representative, one for the EB, one for administrative matters. Mailing list subscription is triggered through emails. To subscribe to a list, a participant must send an email to the Project Coordinator from the email address he/she wants to use in the list. Since the majority of the communication will happen via the plenary mailing list, *senders are invited to identify the matter and work package to which the communication belongs in the subject*. The names of the lists are reported in Table 8.

Name	Purpose
`Secured-all@list.uva.nl`	Plenary mailing lists (excludes only administrative parties)
`Secured-admin@list.uva.nl`	Administrative mailing list (upon request, can include PIs)
`Secured-ga@list.uva.nl`	Representative of each partner in the General Assembly

Name	Purpose
Secured-eb@list.uva.nl	Members of the Executive Board

Table 8 – SECURED Mailing Lists.

The Project Management Team is in charge of updating the consortium members list, which reports, for each consortium member, the contact details, role in the project, mailing lists he/she belongs to, governance bodies participated, and the accesses on the shared repository. The list is accessible by any consortium member at any time, in the shared repository. All partners should periodically check that the list is up to date and promptly communicate to the Project Management Team any change to be applied to the consortium member list (e.g. changes in their contact details or contact persons), as well as of changes in any other information needed for executing the project.

8 Publications, Public Presentations, and Dissemination

When publishing research outcomes that have been supported by SECURED funding, authors should adhere to the dissemination guidelines that are outlined in the SECURED Consortium Agreement, paying particular attention to the notification process. Publications and public presentations must specify that the project has received research funding from the Europen Union. The following statement should appear in a dedicated section or note of the publication or of the presentation material:

> “Funded by the European Union (Grant Agreement Nr. 10109571, SECURED Project). Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the Health and Digital Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.”

Where applicable, authors should also display the appropriated European Union emblem, available at the following address: `https://ec.europa.eu/regional_policy/en/information/logos_downloadcenter` (More information and use examples: `https://ec.europa.eu/info/sites/default/files/eu-emblem-rules_en.pdf`).

Each publication, public presentation of dissemination activity should be promptly reported in the dedicated spreadsheet available on the shared repository. The PDF of the final version of the publication should be also made available to all the partners in the shared repository. The authors should also provide a Digital Object Identifier of the publication to be included in the Dissemination and Communication reports.

9 Risk Management and Conflict Resolution Procedures

Even though the consortium has considerable expertise in EU projects, risks may arise along the technical, financial, managerial, and resources availability dimensions (e.g., unexpected technical difficulties, deterioration of economic situation, partner abandons the project). Severe situations are not foreseen at proposal stage and technical risks are perceived as low due to the high expertise in the consortium.

A detailed list of risks, together with the work packages involved and the possible corrective measures is described in the Description of Actions. In the extreme case of withdrawal of a partner, the corrective measures will include distributing to the remaining partners the activity not fulfilled or to subcontract them to a third party, or a combination of the two. Corrective measures will be chosen after vote of the General Assembly and after an evaluation of their impact and relevance on the project.

Furthermore, to minimize the potential impact in the unlikely case of withdrawal of a partner, the partner in the WP that is not WP Leader and has the highest number of person months will serve as backup WP Leader and will assume WP leader role in case of abandonment.

Several kinds of conflicts can arise in the project, including technical disagreements, strategic divergence, and interest conflicts. Typically, when a dependency between technical components made by different partners exists, a wrong choice in implementation of sub-component will lead to increased cost and financial burden for the partner depending on the component.

The Project Management Team will proactively resolve conflicts, by prioritising smooth cooperation, risk mitigation, and enabling exploitation. The Project Coordinator will resolve technical disagreements in cooperation between the partners to solve dependencies and avoid increased efforts/burdens. Every effort will be made by the Project Coordinator to achieve amicable consensus between conflicting partners.

Project Coordinator will perform day-to-day analysis of the project progresses. In case of problems, they will be reported to the Executive Board that can decide to ask to a specific partner a detailed written explanation of the situation and a contingency plan. Such document will be submitted to the General Assembly for decisions within 10 (ten) working days after the request.

An extraordinary General Assembly meeting will define proper actions in accordance with all partners. In case they cannot agree within reasonable time, the Project Coordinator will have to proactively facilitate the decision, explain the reasons for it to the team, and advise the involved partners in what they should do.

In case of conflicts within a body that cannot be resolved by the leader of this body, the next higher body shall be turned to for the resolution of the conflict. Any conflicts that cannot be resolved through the principles above will be handled according to the dispute resolution provision set forth in the Consortium Agreement.

The foreseen risk, as reported in the Description of Action, are reported in Table 9.

Risk Number	Description	Work Package No(s)	Proposed Mitigation Measures
1	Unforeseen technical problems that may not be resolved with the assigned resources	WP2, WP5, WP3, WP4	The situation will be assessed by the consortium members, in collaboration with the involved WP leaders to decide about adequate re-planning actions that ensure the overall project result.
2	Some developed components are not sufficiently performing	WP2, WP5, WP3, WP4	Careful analysis of user requirements and environmental constraints. Possible replacement with alternative solutions.

Risk Number	Description	Work Package No(s)	Proposed Mitigation Measures
3	Some components are not ready for integration	WP2, WP5, WP3, WP4	The integration process will be progressive and step by step. As soon as an intermediary version of a component is ready, it will be tested in the integration platform. The issues will therefore be solved gradually and not discovered at the end. In addition, early and clear definition of technologies, interfaces and conventions will help to reduce this risk. In addition, emulation of not yet available components by mock-up or simulation can be used. The experimental demonstration could be repeated once the advanced components become available.
4	Difficulties in integration of SECURED components	WP2, WP3, WP4	Careful definition of technical requirements and especially of module interfaces. Consider users' interaction and procedures.
5	The proposed tools not addressing relevant cases.	WP2, WP5, WP3, WP4	Relevant end-users involved in the project from the outset. Sound use cases based on health partners operational experience.
6	Due to system complexity, the integration reduces overall system performance	WP4	Predict and continuously measure module and system performance throughout design, development, and integration activities. Usage of appropriate tools to assess potential shortcoming before the actual integration/deployment of the system.
7	Inability to perform a use case demonstration	WP5	The consortium will take necessary actions in a timely manner, well before the actual use case dates to ensure proper delivery. In the case of a force majeure, the use of appropriate tools can be used for the provision of a synthetic scenario build.
8	SECURED solution is not compliant with GDPR.	WP2, WP1, WP5, WP3, WP4	From the onset of the project in-depth analyses of legal issues in T1.3, T2.5, T4.5 and T5.7.
9	Poor Framework Performance during use case resulting to failure of the use case demonstrations	WP2, WP5	All use case operators will constantly monitor the use case's conditions for such bad performance problems to be depicted at early stages & an adequate and effective solution to the problem to be provided. Moreover, the system developers will study the reasons of the deterioration to find a way to prevent same problems in the future.
10	Poor quality of data to validate the results	WP5	Use cases sites have already been carefully selected to ensure that they are suitable for the demonstrations. T5.1, will analyse the use cases in advance and existing infrastructure to guarantee the requirements during the use case development. In addition, regular remote meetings will be held to check all use cases are aligned with the project.
11	Changes in legislative framework	WP2, WP1, WP5, WP3, WP4	Continuous monitoring and update of possible adoption of new regulations regarding privacy, GDPR and ethics.

Risk Number	Description	Work Package No(s)	Proposed Mitigation Measures
12	Stakeholders outside the project are not interested	WP1	Stakeholders will be contacted early in the project through various communication activities to raise interest throughout the scientific and end user community. One SECURED open call is planned to invite SMEs to try out and experiment with the developed tools.
13	Face to face meetings is not possible due to unexpected events (i.e., COVID-19 pandemic)	WP2, WP1, WP5, WP3, WP4	Online meeting platforms will be used.
14	Partner underperforms or leaves the consortium	WP1	In case of Partner's resignation pending workload will be either re-distributed among Partners based on their competencies or a replacement Partner will be identified. In addition, the Consortium Agreement will foresee such situations and will describe measures to be taken to prevent non-compliance to project activities.
15	Low quality of project results	WP1	The internal reviewing process for all project deliverables and reports, will ensure high quality project results.
16	Data handling: risk to disclose personal and sensitive data	WP1	Legal and ethical procedures will be prepared including security measures.
17	Delays in the tasks' completion due to lack of resources, inability of partners or disharmony in the collaboration	WP1	The work plan of the project has been carefully planned, and the partners have a lot of experience in participating in such projects. Coordinator and project management team will adopt a proactive approach by identifying all critical paths in the project and by performing the necessary rescheduling.

Table 9 – Critical Risks & Risk Management Strategy.

10 Conclusions

This document has set out the practical organization and the procedures of the SECURED project. It is a reference document for the consortium members: all partners must read it and familiarize themselves with it.

The Project Handbook Quality is anyway a work in progress; based on experiences and needs in the consortium, the document will be continuously adapted and updated. Best practice will be incorporated and used to systematically improve the operational management of the project.

A Project Logo

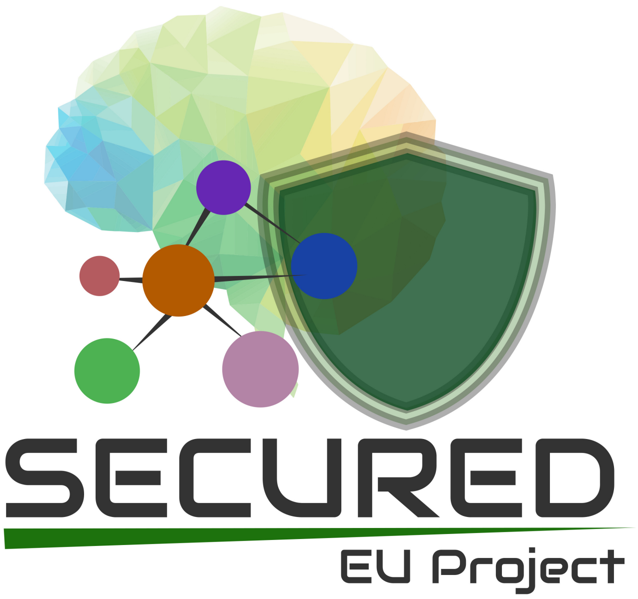

Figure 3 – SECURED Logo