

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



## D1.7 — Project Website



Funded by  
the European Union

Grant Agreement Nr. 10109571

### Project Information

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

### 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 Institutou Systematon 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**

<b>Workpackage</b>	WP1
<b>Workpakace Leader</b>	Francesco Regazzoni (UvA)
<b>Deliverable No.</b>	D1.7
<b>Deliverable Title</b>	Project Website
<b>Lead Beneficiary</b>	ISI
<b>Type of Deliverable</b>	Report and Demo
<b>Dissemination Level</b>	Public
<b>Due Date</b>	31/03/2023

**Document Information**

<b>Delivery Date</b>	23/03/2023
<b>No. pages</b>	26
<b>Version   Status</b>	1.0   final
<b>Deliverable Leader</b>	Christos Tselios, Evangelos Haleplidis, Apostolos Fournaris (ISI)
<b>Internal Reviewer #1</b>	Daniela Spajic, KUL
<b>Internal Reviewer #2</b>	Anastasia Vayona, CEF

**Quality Control**

<b>Approved by Internal Reviewer #1</b>	30/03/2023
<b>Approved by Internal Reviewer #2</b>	30/03/2023
<b>Approved by Workpackage Leader</b>	03/04/2023
<b>Approved by Quality Manager</b>	05/04/2023
<b>Approved by Project Coordinator</b>	06/04/2023

### List of Authors

Name(s)	Partner
Christos Tselios, Evangelos Haleplidis, Apostolos Fournaris	ISI

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	Apostolos Fournaris(ISI)	Created the document and the initial version of its content
03.03.2023	0.2	Christos Tselios, Evangelos Haleplidis, Apostolos Fournaris (ISI)	Added deliverable text
06.03.2023	0.3	Evangelos Haleplidis	Provided additional input to the text
15.03.2023	0.3	Christos Tselios, Apostolos Fournaris (ISI)	Provided final version

## Table of Contents

---

<b>1</b>	<b>Executive Summary</b>	<b>7</b>
1.1	Related Documents . . . . .	7
<b>2</b>	<b>Introduction</b>	<b>8</b>
2.1	Structure of the Document . . . . .	8
<b>3</b>	<b>Project Logo</b>	<b>9</b>
<b>4</b>	<b>The Project Website</b>	<b>10</b>
4.1	Structure and Scope . . . . .	10
<b>5</b>	<b>Website Layout and Sections</b>	<b>11</b>
5.1	Home . . . . .	11
5.1.1	Project Scope . . . . .	11
5.1.2	Objectives . . . . .	12
5.1.3	Pilots . . . . .	12
5.1.4	Bottom of the page - Footer . . . . .	14
5.2	SECURED Innohub . . . . .	14
5.3	Concept and Architecture . . . . .	15
5.3.1	Project Wiki . . . . .	16
5.3.2	Consortium . . . . .	18
5.4	News and Events . . . . .	19
5.5	Contact . . . . .	19
5.6	Open Call . . . . .	20
<b>6</b>	<b>Social Media</b>	<b>21</b>
<b>7</b>	<b>Dissemination Monitoring</b>	<b>24</b>
<b>8</b>	<b>Conclusions</b>	<b>25</b>

# 1 Executive Summary

---

The project website represents one of the major means of dissemination, outreach and communication with the external stakeholders and the general public. It is, therefore, a critical channel for broadcasting the overall progress of project, namely project updates, news, related events, submitted papers and other scientific results. The website along with the already created social media will facilitate creating awareness for the project, visitor and audience interaction with the consortium members and will play a vital role for promoting the project outcomes. The current document contains the description of the initial version of the SECURED project website, which will be updated during the duration of the project and will remain available for 2 years after the end of the project. The main objective of this document is to provide a detailed description of the website which has been set up according to plan at M3 of the project and will be progressively updated and expanded throughout the three-year project lifecycle. The current version of the website already contains initial information about the project, its objectives, the project partners, concept, approach, use cases etc. Furthermore, in this document, we present the four social channels which will be used for complementing all dissemination activities in parallel with the project website. Additionally, we provide some information regarding the Project's Wiki which will act as the main public document repository and will be also maintained by the project dissemination leader, ISI.

## 1.1 Related Documents

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

## 2 Introduction

---

This report comprises the project's Deliverable D1.7 "Project Website" that is associated with the T1.4 "Dissemination Activities, Training and Education Activities and Planning". As described in the Grant Agreement, this task organizes the transfer of knowledge and of project results, both within the consortium and to the outside world. It ensures that all involved organizations are kept informed and can promote project results. Thus, the interactive and online (professional social networks and project's website) dissemination channels are considered of particular importance for influencing prospective adopters of the SECURED framework. The aim of this task is to widely disseminate and present the SECURED project's [1] outcomes to the scientific and technical communities. The first step for doing so is the creation of the SECURED website that will operate as the forefront of the overall SECURED ecosystem. The website (portal) will act as the main reference point, centralizing the scientific results, standard documents and all bits of contextual information regarding the SECURED project. All appropriate dissemination material such as leaflets, brochures, posters, flyers, newsletters, posters as well as public deliverables and other project-related material will be available on the project website. Furthermore, the website will include feeds from the associated social media which will provide live updates of the project participation in public events, key achievements, pilot results etc. The project's website is accessible at the address <https://secured-project.eu/> and is designed to be simple, functional and intuitive not only for the project's stakeholders but all types of audience. Currently the website contains a brief description of the project including the project objectives, concept and approach, some information about the consortium, as well as the latest news feed located in a separate section. The dissemination leader, with the help of the rest of the partners, will be constantly updating the content and dynamically enriching the available material throughout the duration of the project, covering the project's progress and relevant activities. This website is hosted by ISI, the consortium's dissemination leader, while the rest of the partners will contribute to its different sections by providing updates on results, publications, news and events, as the project progresses.

### 2.1 Structure of the Document

Section 2 gives the reader a detailed view about the project website <https://secured-project.eu/> by describing each specific subsection/webpage. For instance, Section 2.1 provides information about the website's structure and scope, while Section 2.2 gives a view of the Website Layout and Sections. More specific, the reader can obtain information regarding the Home page design (Section 2.2.1), the SECURED Innohub (Section 2.2.2) as well as get an insight of the overall Project Concept and Architecture (Section 2.2.3). Additional sections contain information regarding News and Events (Section 2.2.4), Contact functionality (Section 2.2.5) as well as the Open Call (Section 2.2.6). The document continues in Section 3 with the "Social media" section where we describe the social media platforms, where the SECURED Project will have a presence, and Section 4 refers to the "Dissemination Monitoring" where certain KPIs are listed. Finally, Section 5 contains the conclusions and provides a summary of the information reported in the deliverable.

More specific, this document is divided as follows:

- A short introduction describing the website structure.
- The outline of the website, providing a description of each section. In particular, the most important ones are: Home Page, SECURED Innohub, Concept and Architecture, Project Wiki, Consortium, News and Events, Contact and Open Call.
- Information about the Project Wiki created as the main point of reference for public documentation, such as public deliverables, reports and scientific papers.
- Social media presence –social media channels.
- Dissemination monitoring strategy, where the tools and KPIs to be used for performance monitoring are being suggested.
- The conclusion section.



### 3 Project Logo

---

The logo is a key element of the overall SECURED Project dissemination material which aims to provide a concrete project identity. The scope of its design is no other than to capture the concept behind the SECURED project, and the context of its use cases which navigated the description of the Pilots and defined the expected results. The logo has been created by the dissemination leader (ISI) at the beginning of the project and all project templates will be based on it (deliverables, poster, presentation and internal reports as well). The logo will be used for any dissemination activity and created content.



Figure 1 – The SECURED Project Logo

## 4 The Project Website

### 4.1 Structure and Scope

As stated in Section 1, the website contains all the essential information concerning the project and will be constantly updated with produced material, news, photos, etc. The main goals of the website are to present the project's progress to the scientific, academic and technical communities, and overall, to promote and make visible the intermediate and final outcomes to the general public, thus facilitating collaboration between the project partners, stakeholders and the rest of the audience. The website is designed to be easily accessible and user friendly to its potential visitors. It will remain available for 2 years after the project ending and the partnership will take any necessary measures in order to ensure that the results will be widely available, open and accessible to the public through additional mediums for a considerable length of time. The SECURED project website has been developed and published at M3 of the project according to schedule. The domain is <https://secured-project.eu/> and was registered by the dissemination leader, ISI, in collaboration with a Greek company, Enartia MEPE.

Figure 2 below presents the initial website map (menu structure). Figure 2 provides a tree diagram representing the website structure

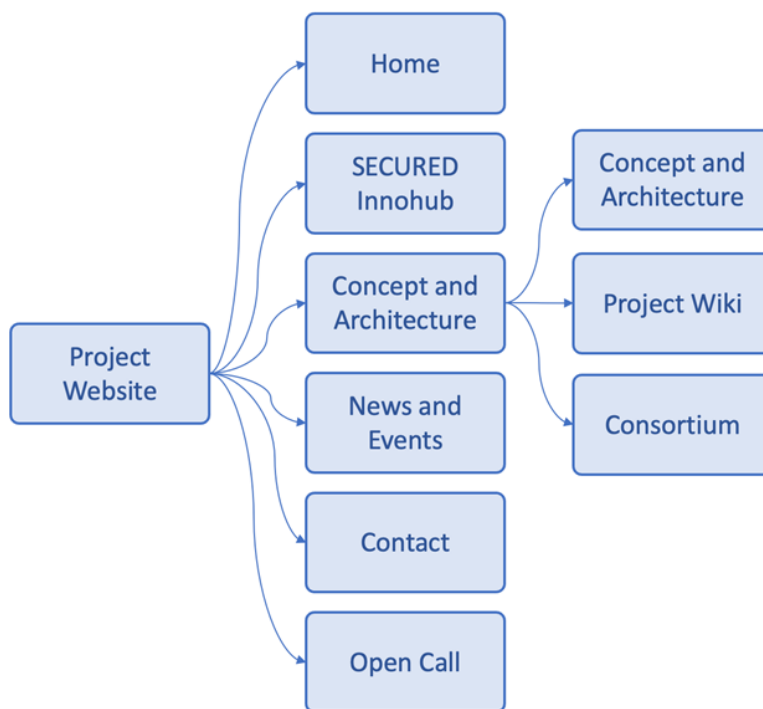


Figure 2 – Tree diagram representing the website structure

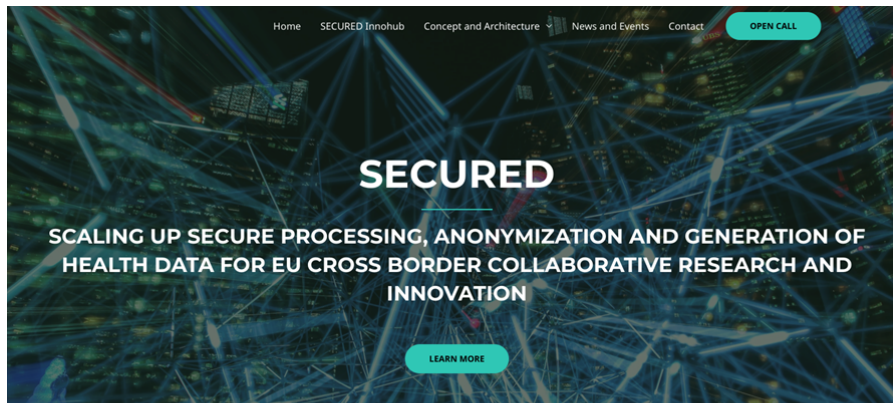
ISI will be responsible for the website hosting, management, data handling, maintenance, upgrades/updates, and any further changes needed in terms of content and appearance. Partners are encouraged to provide content to the dissemination leader that will decide along with the project coordinator whether the content will be uploaded on the website. Modifications and/or improvements are likely to be identified in the future to address any requirements not identified at this early stage of the project. The Project Wiki area is seamlessly integrated into the website and will be also maintained by ISI.

## 5 Website Layout and Sections

### 5.1 Home

The Home page which is presented in [Figure 3](#) is the gateway to the main website sections. The Home page provides to the viewer a preview of all the sections in a slide form and represents a user friendly and easy interface to the visitors for navigation

The Home page is organized according to the following design model:



In SECURED, we offer a one stop collaboration hub (the SECURED Innohub) that can provide a secure and trusted environment for decentralized, cooperative processing of health data through SMPC techniques as well as generation of new, synthetic data and anonymization and anonymization assessment to health data providers and users. Our vision is to facilitate the broad adoption of health datasets across Europe by making the interconnection between EU health data hubs, the health data analytics research community, health application innovators

**Figure 3** – Top of the Page

The Home page menu items include:

- Home
- SECURED Innohub
- Concept and Architecture
- News and Events
- Contact
- Open Call (up right)

#### 5.1.1 Project Scope

The scope of the project is clearly described on the top of the website.

Since the overall goals of the SECURED project include (i) multiparty computation scale-up, (ii) data anonymization and synthetic data generation while increasing efficiency and improving security (iii) focusing on private and unbiased artificial intelligence and data analytics and last but not least (iv) cross-border cooperation of health-related data and data hubs, it becomes essential to describe the notion of the SECURED Innohub.

The SECURED Innohub is a single stop collaboration hub which will provide a secure and trusted environment for decentralized, cooperative processing of health data through Secure Multiparty Computation (SMPC) techniques as well as generation of new, synthetic data and anonymization and anonymization assessment to health data providers and users. The project's vision is to facilitate the broad adoption of health datasets across

Europe by making the interconnection between EU health data hubs, the health data analytics research community, health application innovators (like Healthcare SMEs) as well as end users, rendering the SECURED Innohub a fundamental element toward realizing this vision.

### 5.1.2 Objectives

A well-defined project objective describes a status, which should be achieved at the end of the project, optimally quantified in terms of quality, time and cost. As objectives are necessary for planning, monitoring and proper project control, it is essential that all project stakeholders have a clear understanding of tasks, expectations and necessary steps toward success.

The objectives subsection of the SECURED Project website Home page contains the 8 project objectives in order to enhance clarity and deliver the essential context of what exactly the consortium tries to achieve (see Figure 4).

In SECURED, we offer a one stop collaboration hub (the SECURED Innohub) that can provide a secure and trusted environment for decentralized, cooperative processing of health data through SMPC techniques as well as generation of new, synthetic data and anonymization and anonymization assessment to health data providers and users. Our vision is to facilitate the broad adoption of health datasets across Europe by making the interconnection between EU health data hubs, the health data analytics research community, health application innovators (like Healthcare SMEs) as well as end users. The SECURED Innohub is offering apart from an SMPC and anonymization framework (with appropriate tools and services), the means to engage its members in the EU health data community by providing training and well as synthetic data to stem health data analysis research, medical education and an increase of the associated datasets volume and considerably reduce their bias. The SECURED vision is to kick start an EU cross-border health data collaboration ecosystem for data providers, data researchers and innovators that will be able to produce new AI based data analytics solutions and stem innovation.



Figure 4 – Project Scope and part of the Objectives Section, as seen from the Home page

### 5.1.3 Pilots

This subsection provides to the visitors some information on the four pilots of SECURED project (see Figure 5, namely

- Real-Time tumor classification, led by Erasmus Medical Center
- Telemonitoring for children, led by Paediatric Hospital Nino Jesus
- Synthetic Data generation for education, led by Semmelwies University
- Access to Genomic Data, led by JCLRI

### SECURED PILOTS



**Pilot 1 (Erasmus Medical Center): Real-Time tumor classification**

Using the SECURED architecture, this pilot expects using Ultrasound and Brain imaging to generate novel insights related to the correlation of anatomically separate but functionally connected brain regions, confirmations of previous connectivities and discovery of new ones.



**Pilot 2 (Paediatric Hospital Niño Jesús): Telemonitoring for children**

Using the SECURED architecture, this pilot expects, in terms of prediction of bad evolution in oncology patients, the capability of using AI will foster the extension of telemedicine among paediatric patients, which can contribute significantly to meet goals 1, 3, 13, and 15 of 2030 Agenda for Sustainable Development.



**Pilot 3 (Semmelweis University): Synthetic-data generation for education**

Using the SECURED architecture, this pilot expects to facilitate movement between countries and statistical data collection while protecting individual privacy, generate large amounts of synthetic data guaranteed to be GDPR compliant, educate doctors get a quick overview of millions of cases due to machine learning data synthesis instead of generalising from a single cases and finally doctors integrate machine learning tools into their daily practice.



**Pilot 4: (JCLRI) Access to Genomic Data**


During this pilot, SECURED's federated learning system will allow researchers to train their models on all existing genetic data without the need of spending months preparing the paperwork to access it while, at the same time, preserving patient privacy, will transform the way genetics research is currently done.

Figure 5 – Secured pilots as appear in the Home page

This section will be further expanded during the project course to provide more information and updates regarding the two pilot use cases.

In order to enhance user friendliness, the Home page also contains a “Latest News and Events” as well as a “Social Media” subsection (see Figure 6). These two subsections were deliberately placed into the Home page in order to provide the most updated information regarding SECURED project activities, without forcing the user to navigate into the relevant sections of the website or the social media platform.


### LATEST NEWS AND EVENTS



**SECURED Kick off Meeting in Amsterdam**

The kick - off of the SECURED project took place at the University of Amsterdam premises in Amsterdam on the 25th and 26th of January 2023.

[LEARN MORE →](#)




**SECURED project starts!!**

On January 2023 the SECURED project started a journey to provide innovative solutions for cross-border collaboration of Health data hubs using secure multiparty, privacy preservation and synthetic data generation approaches.

[LEARN MORE →](#)

### SOCIAL MEDIA



Tweets from @SecuredEU

Secured EU Project @SecuredEU - Mar 10  
Let's meet and start collaborating ... The very fruitful kick-off meeting of the SECURED EU project was held in Amsterdam at the UvA premises on January 25th and 26th. Excellent discussions and planning!

Secured EU Project @SecuredEU - Mar 14  
SECURED EU Horizon Europe project has officially started. Stay posted for upcoming updates #Privacy #Security #EUprojects

[View more on Twitter](#)



Figure 6 – Latest News and Events / Social Media snippets, as appear in the Home page

Finally, at the bottom of the website, right before reaching the footer, the visitor may find some preliminary information about the SECURED Project consortium (see Figure 7).



Figure 7 – Consortium Partners in the Home page

### 5.1.4 Bottom of the page - Footer

The footer area, as seen in Figure 8, contains the relevant EU funding information, the project grant agreement number and additional information regarding the project and its coordinator. The footer also contains the social media (“follow us”) buttons for redirecting viewers to the project’s social media channels, namely Facebook, Twitter, LinkedIn, and YouTube, as seen in Figure 9. Similar with the header area, the footer is visible by all the pages of the website.

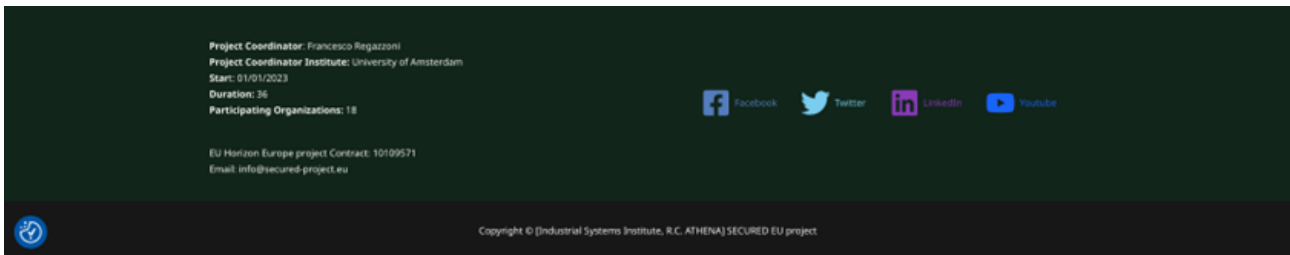


Figure 8 – Bottom of the page – Footer

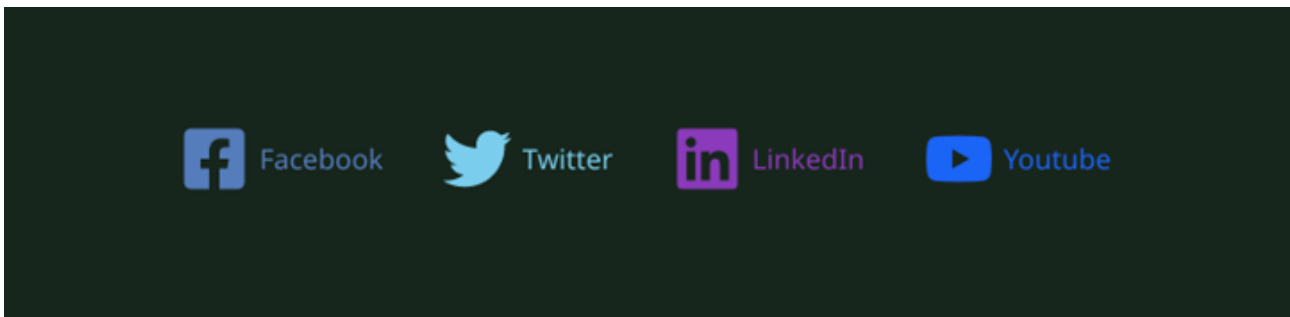


Figure 9 – Social media buttons

## 5.2 SECURED Innohub

The “SECURED Innohub” section follows the “one-pager” design principle to broadcast large chunks of information in the most user-friendly manner. After accessing the main area, the user simply needs to scroll down and consume information related to the SECURED InnoHub, a Privacy-enhancing Hub that will provide tools, services, and overall support to externally involved third parties of the healthcare domain, including researchers, innovators or health data users as well as data hubs across Europe, thus facilitating them to perform accurate data analytics in a distributed and private matter. A preliminary draft of the SECURED InnoHub functionality is also available, as shown in Figure 10 and Figure 11.



# SECURED CONCEPT AND ARCHITECTURE

## CONCEPT

In SECURED, we offer a one stop collaboration hub (the SECURED Innohub) that can provide a secure and trusted environment for decentralized, cooperative processing of health data through SMPC techniques as well as generation of new, synthetic data and anonymization and anonymization assessment to health data providers and users. Our vision is to facilitate the broad adoption of health datasets across Europe by making the interconnection between EU health data hubs, the health data analytics research community, health application innovators (like Healthcare SMEs) as well as end users. The SECURED Innohub is offering apart from an SMPC and anonymization framework (with appropriate tools and services), the means to engage its members in the EU health data community by providing training and well as synthetic data to stem health data analysis research, medical education and an increase of the associated datasets volume and considerably reduce their bias. The SECURED vision is to kick start an EU cross-border health data collaboration ecosystem for data providers, data researchers and innovators that will be able to produce new AI based data analytics solutions and stem innovation.

The SECURED overall approach follows two parallel, independent yet interacting flows to innovation, the data flow and the processing flow, as seen in Figure 1.

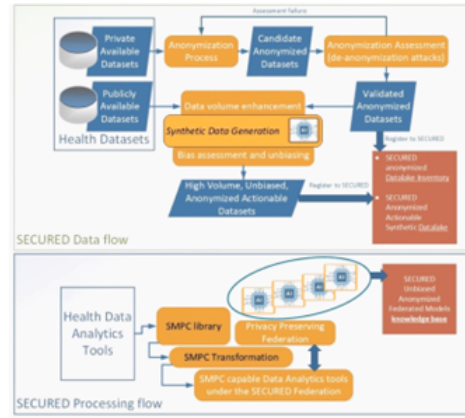
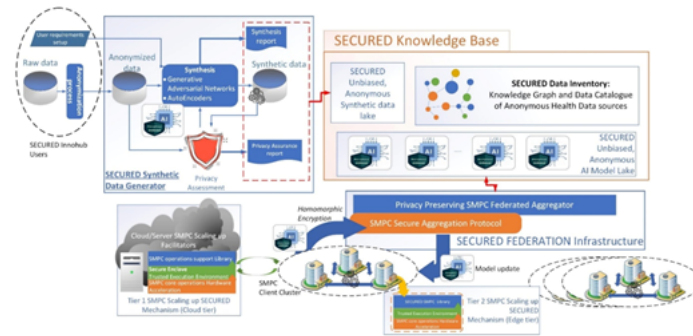


Figure 12 – SECURED Project Concept

## ARCHITECTURE



Project Coordinator: Francesco Regazzoni  
 Project Coordinator Institute: University of Amsterdam  
 Start: 01/01/2023  
 Duration: 36  
 Participating Organizations: 18

[Facebook](#)
[Twitter](#)
[LinkedIn](#)
[Youtube](#)

EU Horizon Europe project Contract: 10109571  
 Email: info@secured-project.eu

Copyright © [Industrial Systems Institute, R.C. ATHENA] SECURED EU project

Figure 13 – Project Architecture

### 5.3.1 Project Wiki

The Project Wiki subsection was designed to become the SECURED Project’s main point of reference for accessing all public documentation, such as public deliverables, reports and scientific papers. All details about the authors, titles and the conferences/journals/workshops will be also given for each publication with the related



links. The provided publications will also be properly archived.

The Project Wiki is further divided into the following sub-sections:

- Publications (under this sub-section we will release research papers, journal articles, concept notes, whitepapers etc).
- Public Deliverables, according to the definition of the work formally agreed with the European Commission, will be limited to the project deliverables where the dissemination level is set to “public”, which will be further categorised per Work Package.

Figure 14 and Figure 15 present the current structure of Project Wiki before adding publicly available content.

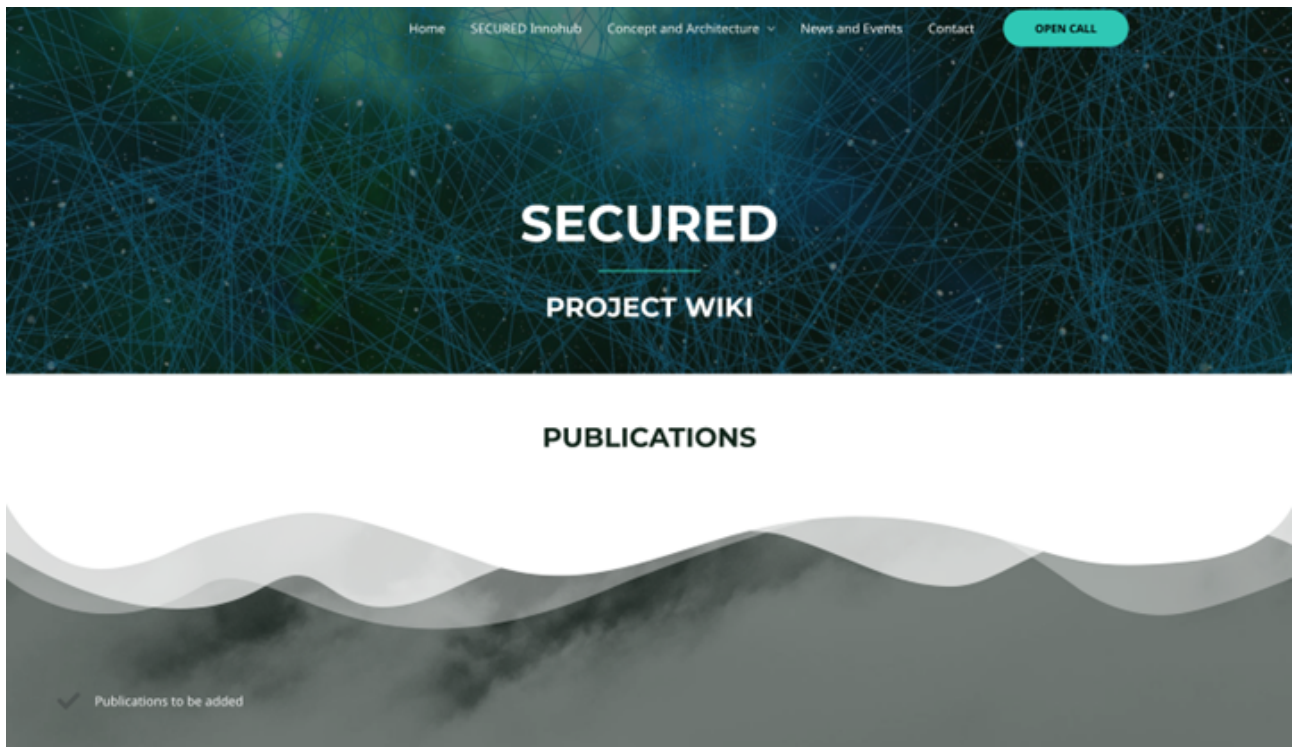


Figure 14 – Project Wiki – Publications subsection

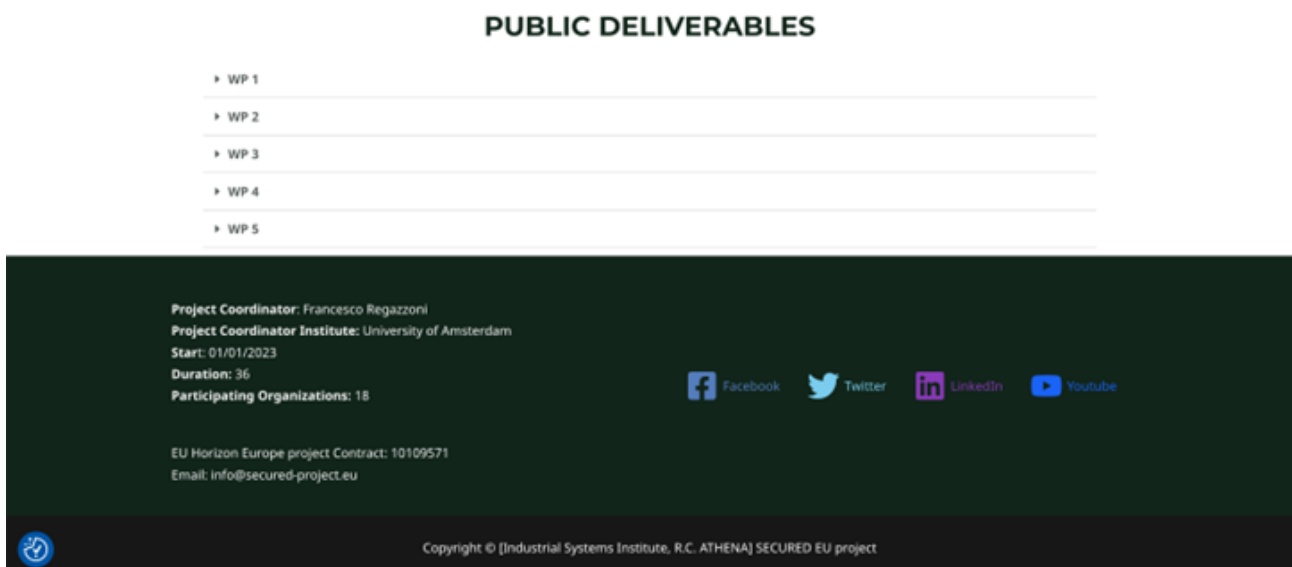


Figure 15 – Project Wiki – Public Deliverable subsection

### 5.3.2 Consortium

The SECURED “Project Consortium” subsection found in the Home page, presents each partner of the Consortium and will be updated to allow the website visitor to connect to the partner’s respective official website (see Figure 16). The SECURED consortium brings together a formidable array of eighteen (18) experienced, highly talented and committed partners from across Europe. Clinical excellence comes from the Erasmus Medical Centre, Netherlands and Hospital Nino Jesus and Josep Carreras Leukaemia Research Institute, Spain. The consortium covers a broad spectrum of security and privacy specialists from embedded systems (UvA, EMC, ISI), law and ethics experts (KU Leuven), security and privacy hardware and software designers (NXP, UvA, ISI, EMC, ATOS, THALES), privacy protocol designers (UCC, NXP), federated learning experts (BME, NXP, HNJ, ICCS), data anonymization specialists (UCC, NXP, ATOS), synthetic data generation tool developer (BSC, THALES, BME) and formal verification analysts (UNISS). Global IT & services companies (THALES, ATOS, NXP) bring highly relevant industry experience and expertise in artificial intelligence, private computation and anonymization technologies. Catalink, an innovative SME, brings expert knowledge in the integration of complex systems, while CEF, also an SME, will lead the funding call to provide direct support to health technology SMEs outside the consortium to include technologies researched in the project. Industrial partners ATOS, NXP, THALES, CTL all have a clear mandate to exploit project outputs in the privacy technologies and AI markets.

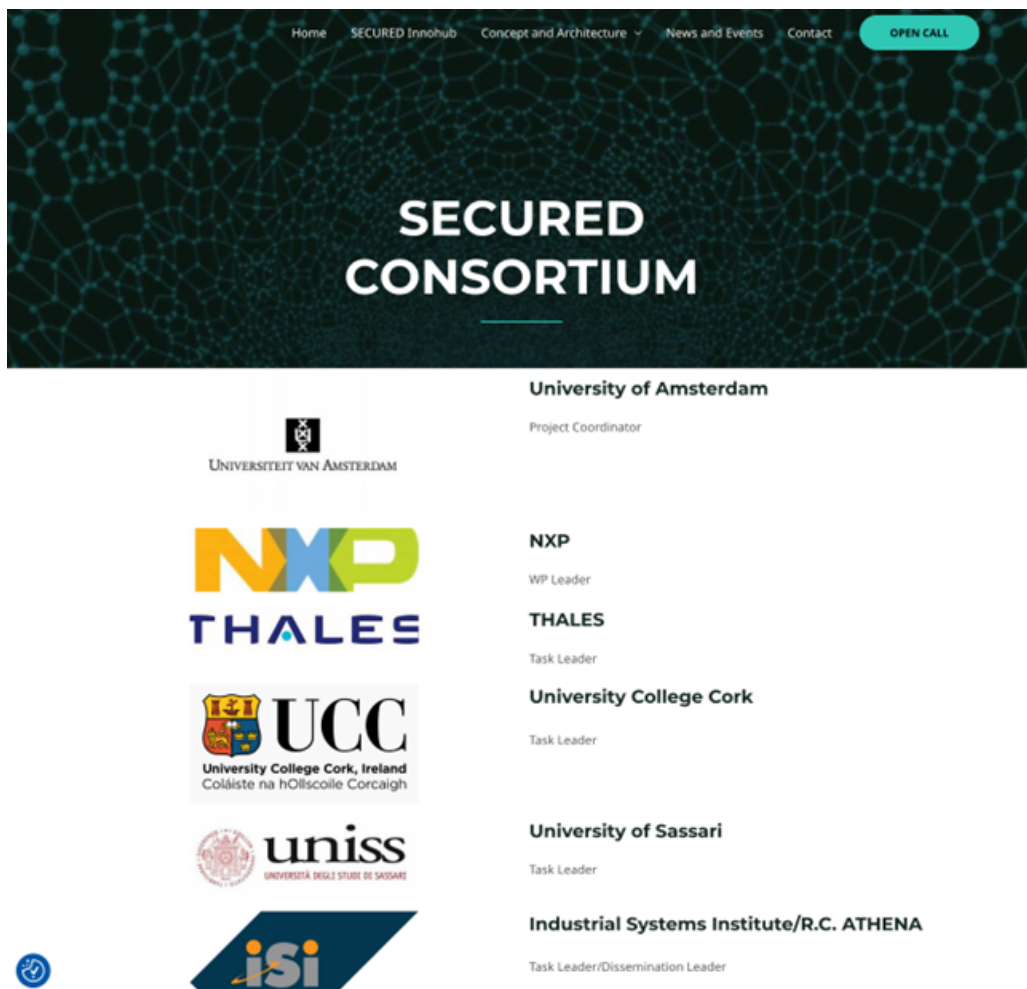


Figure 16 – Project Consortium Section

## 5.4 News and Events

The “News and Events” section presents the latest project updates and, as the rest of the website (see [Figure 17](#)), this section will also be constantly updated with information such as upcoming plenary meetings, technical workshops, participations in events, synergies with other projects, demonstrations, conferences, publications, whitepapers, newsletters, papers, etc. Currently it includes two posts along the related photos. Any post in this section can be visible in the side bar of the website as displayed in [Figure 17](#).

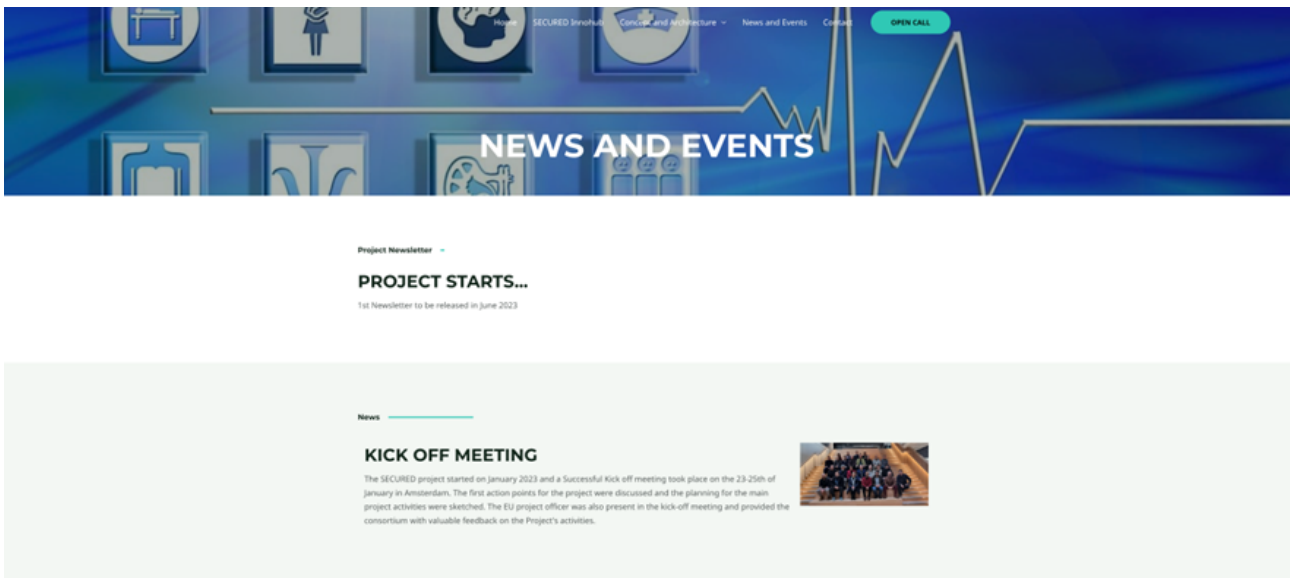


Figure 17 – News and Events section

## 5.5 Contact

In order to facilitate communication with the project stakeholders, a dedicated contact form was developed. Website visitors will be able to submit questions, ideas, comments and generic messages to the project's consortium, in an automated and easy to use manner (see [Figure 18](#)).

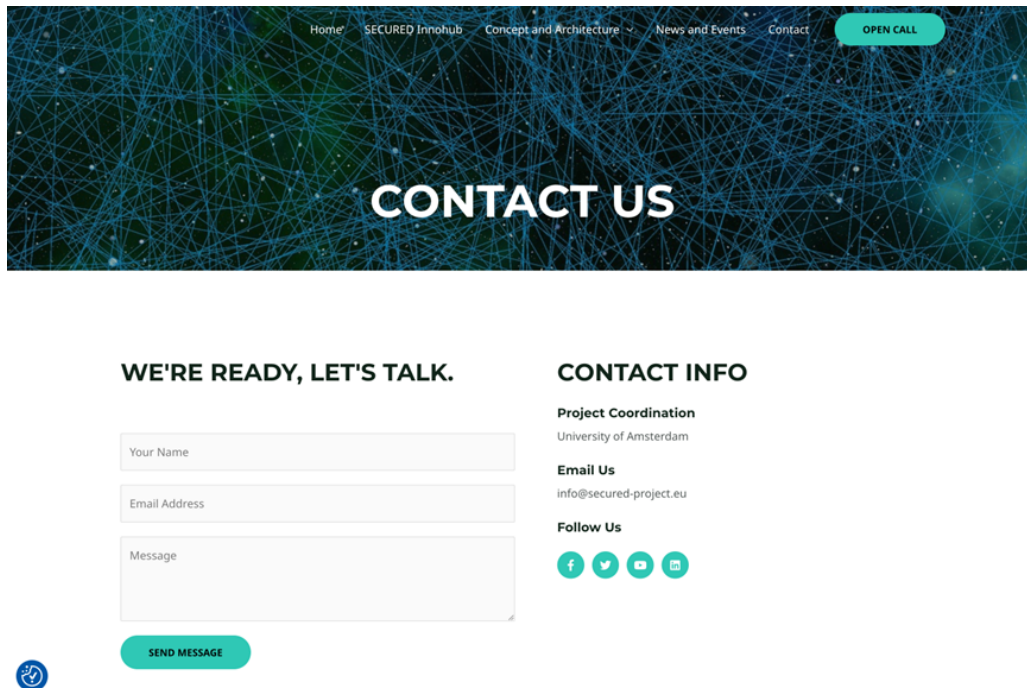


Figure 18 – Contact us section

## 5.6 Open Call

The SECURED Project intends to promote the interaction of external third parties employing AI solutions with SECURE Innohub, via a dedicated Open Call.

The aim of the Open Call is threefold:

- To validate the developed solutions with Healthcare and AI stakeholders external to the consortium in order to test the efficacy and applicability of our proposed solution.
- To seek out external AI / ML stakeholders, data providers, research teams and SMEs with expertise on AI medical applications, medical data handling, technical/security tools providers and datasets holders for sharing and advancement of knowledge.
- To raise awareness of the project's activities and encourage participation by a broad community in order to keep up the momentum of the project's ambitions even after its completion.

For promoting the Open Call, the SECURED Project website contains a dedicated area that will encompass all related information and will be populated with content in the next few months.

## 6 Social Media

The project's online presence will be complemented with a strong social media presence, as dissemination nowadays through Social Networks is essential. Already a Facebook page, a Twitter account and a LinkedIn page have been created for communicating project achievements to a wider audience. Social media channels, such as Twitter, can be effective in communicating project announcements while LinkedIn and Facebook can be effective in promoting discussion, spurring interest in and generating awareness of the project and its associated activities.

- The Facebook page channel (Figure 19) has been set up to spread information to the general public. A Facebook page was created under the link <https://www.facebook.com/securedEUproject/>. This social media will be used for public project communication in the form of text, pictures and videos from project meetings as well as disseminations activities such as participation and presentation in conferences, attendance in forums etc.
- The Twitter page (Figure 20) will be used for communication with related stakeholders and actors through networking, short updates on project news (tweets) and announcement of upcoming or completed activities. A Twitter account (<https://twitter.com/SecuredEU>) has been created in order to share with the large twitter community all the news related to the project. All "tweets" will be posted by the dissemination leader and the appropriated functionality was integrated into the website for the tweets to be visible in real time.
- The LinkedIn page (Figure 21) is appropriate for providing updates for the project progress targeting mainly the professional networks and communities of LinkedIn. The project's LinkedIn page is accessible at <https://www.linkedin.com/company/secured-project/>
- The YouTube channel (Figure 22) will be populated with the relevant research activities and pilot-related videos to further broadcast SECURED project pilots, synergies as well as their benefits for end users and stakeholders. The YouTube channel is currently without content, yet accessible at <https://www.youtube.com/@securedEUproject>

All social media channels will be updated regularly by the dissemination leader in order to ensure that the content is current and accurate and will include all relevant information, photos and updates on the project's on-going activities. Moreover, the YouTube channel will be populated with the relevant research activities and pilot-related videos. Video material on YouTube will aim at explaining in an accessible way how SECURED technologies work and what are the benefits for the end users and other stakeholders. As for Facebook, LinkedIn and Twitter, direct links are already visible in each website's section by means of their characteristic icon.

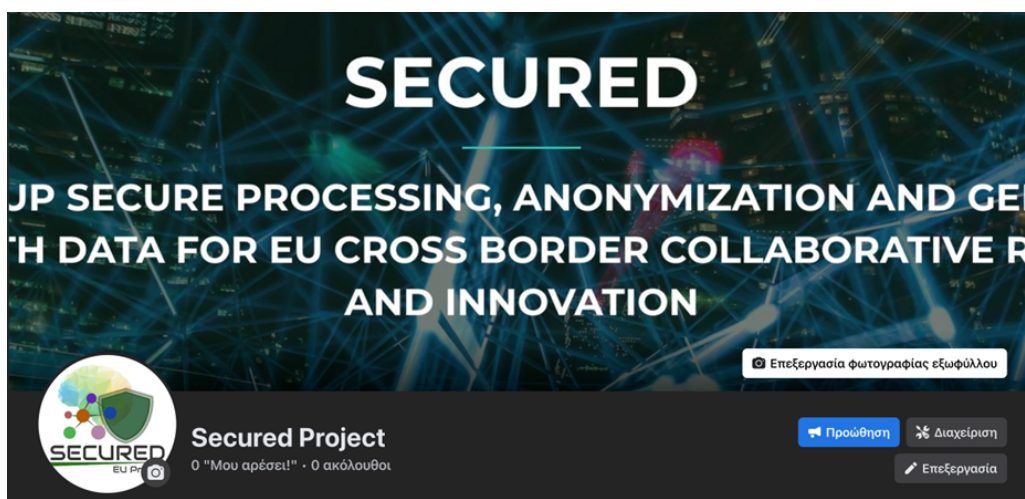


Figure 19 – Project presence on Facebook

The image shows a screenshot of the Twitter profile for the Secured EU Project (@SecuredEU). On the left is a navigation menu with options: Home, Explore, Notifications, Messages, Bookmarks, Twitter Blue, Profile, and More. Below the menu is a blue 'Tweet' button. The profile header features a circular diagram titled 'Secured EU Project' with 'SECURED Federation infrastructure' at the center. Surrounding this are 'TOOLS' (Data Anonymization Client, MPC, ML/DL, PI library, Data De-Anonymization based Privacy Assurances, Secure MPC Tool Transformer, Synthetic Health Data Generator) and 'SERVICES' (Synthetic Data Generator, Secure MPC Followed Training, Health Data Hubs, Legal and Ethics, EU Legislation, National Legislation, Legal Partner). Other elements include 'Good Practices' (Beta testing, Tools/services, Ecosystem buildup), 'Research Entities' (Health4Star), and 'Health4Star' logo. The profile bio states 'Secured EU Project @SecuredEU', 'Joined March 2023', '3 Following', and '8 Followers'. A tweet from March 16th reads: 'Let's meet and start collaborating .... The very fruitful kick-off meeting of the SECURED EU project was held in Amsterdam at the UvA premises on January 25th and 26th. Excellent discussions and planning!' and includes a group photo of approximately 20 people on a staircase. The tweet has 1 reply, 1 like, and 36 retweets.

Figure 20 – Project presence on Twitter

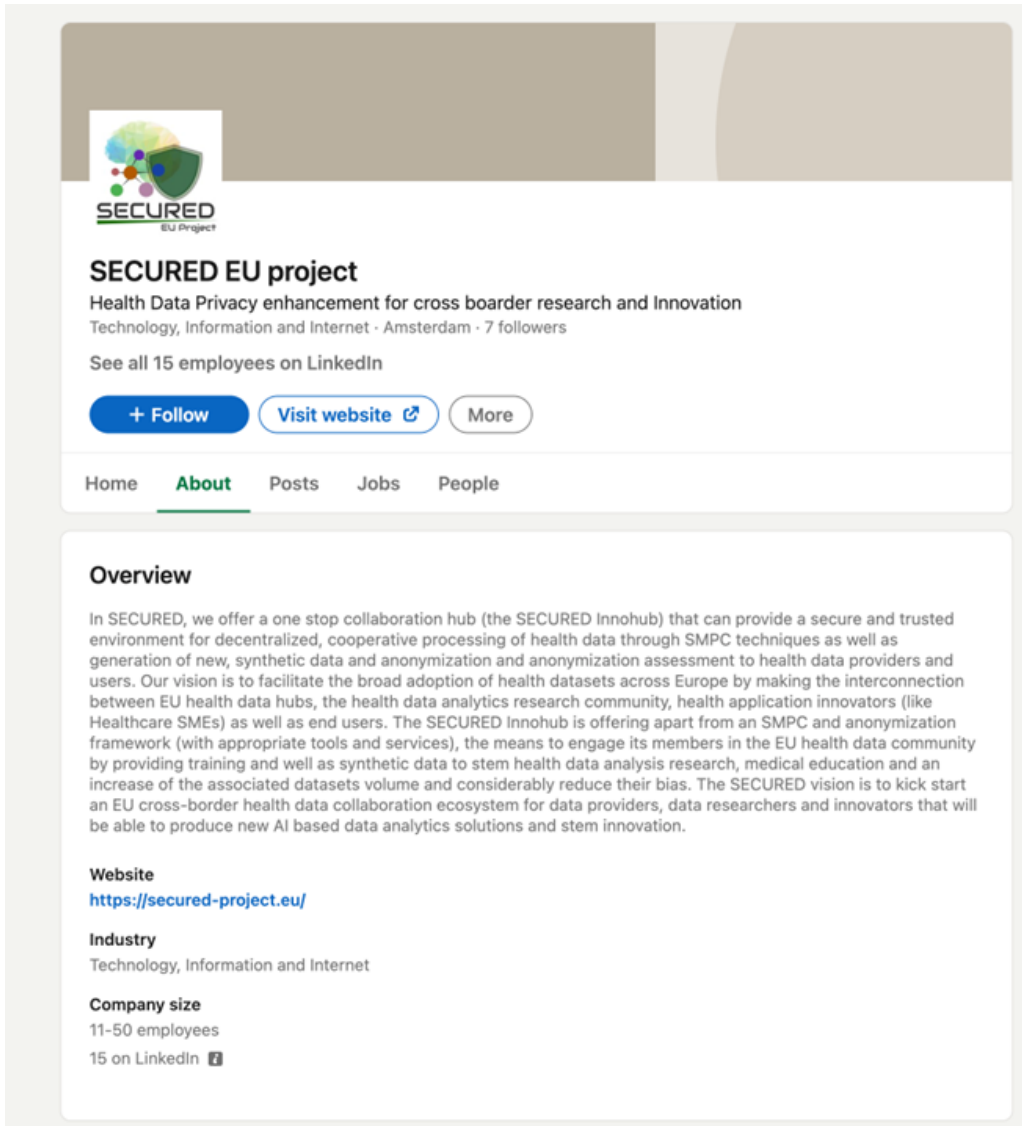


Figure 21 – Project presence on LinkedIn

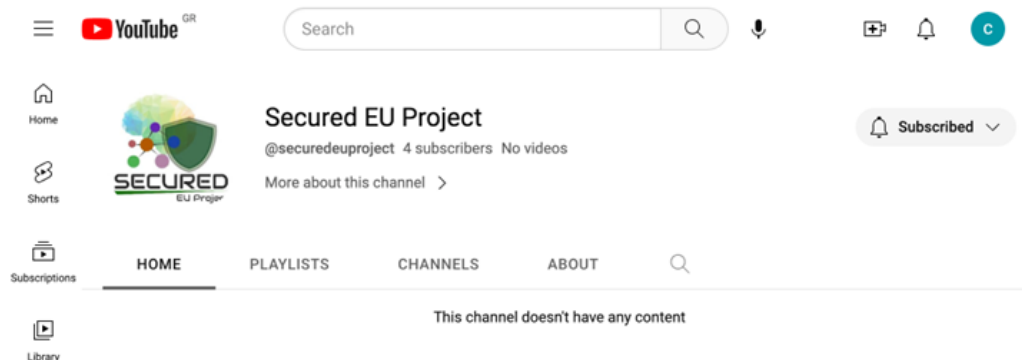


Figure 22 – Project presence on YouTube

## 7 Dissemination Monitoring

---

Dissemination outreach will be measured by internet hit statistics on website, attendance of events and other statistical methods of the chosen dissemination channels.

The website will produce measurement of web traffic based on web analytics. The aim is to measure the digital impact of the project, through the collection of information like bounce rate, number of visitors per day, month, visitors per country, returning visitors, most visited sections, used devices and browser for entering the website etc.

Some KPIs considered for monitoring the project website are the following ones:

1. Number of visitors
  - per day
  - per month
  - per year
2. Visitors' country
3. New and returning visitors
4. Bounce rate: It represents the percentage of visitors who enter the site and then leave ("bounce") rather than continuing to view other pages within the same site. Bounce rate is calculated by counting the number of single page visits and dividing that by the total visits. It is then represented as a percentage of total visits
5. What types of devices they use to access the website (mobile, tablet etc)
6. What type of browser do the users use for entering the website
7. Visited pages: Most popular sections
8. Pages per visit: How many pages are being visited on average (per visit)
9. Average visit duration: How much time do visitors spend on a page
10. Number of new subscribers



## 8 Conclusions

---

In a nutshell, the current document includes a detailed description for the SECURED project website, which in its current state is considered sufficient for the preliminary dissemination of project progress and outcomes, as well as for promoting some initial activities. The current design is considered as a starting point and will evolve during the project reflecting the progress and development on the different use cases and work packages. The website will be regularly updated by the responsible partner ISI in collaboration with the rest of the partners to reflect the latest project updates, relevant results and breakthroughs. It will remain also available for 2 years after the project's end. Sections and content will be continuously updated and progressively elaborated as the project lifecycle moves on and the objective is to expand the sections and if needed to add new sections. For instance, in the Project Wiki, scientific papers and public deliverables will be uploaded and will be available for downloading. Moreover, the news area will be updated with upcoming events and information, photos, partners' activities etc. Graphic layout will be maintained simple in order to be user friendly and easily accessed by any visitor. As mentioned, we will use available tools for monitoring KPIs regarding the website traffic and already a list of potential KPIs is under study. The dissemination leader will maintain and review the website performance trends and along the rest of the consortium will engage into corrective or optimisation actions to increase the impact of the website. Additionally, all partners are committed to advertise the project website during the various dissemination activities they will be participating into as well as through their institutions' social media. Finally, the use of three of the most popular social networks will facilitate information exchange and interaction with other interested stakeholders and will help to establish synergies with other projects as well as various scientific communities. Without a doubt, the project website remains the main dissemination channel, yet, we anticipate that social networks will facilitate broadcasting the SECURED project results to a larger audience in both business and academia.

## References

---

[1] "SECURED cordis announcement," <https://cordis.europa.eu/project/id/101095717>, accessed: 2023-01-01.