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

Annex 2

SECURED OPEN CALL GUIDELINES FOR APPLICANTS

This document is published in the context of and for the objectives of the SECURED project. The SECURED project has been financially supported by the European Union through the HORIZON-HLTH-2022-IND-13 (HORIZON-RIA) under Grant Agreement No. 101095717

Table of Contents

1 Introduction

This document serves as the guideline for applicants applying to the Scaling Up Secure Processing, Anonymization And Generation Of Health Data For EU Cross Border Collaborative Research And Innovation (SECURED) - Open Call, providing comprehensive information and participation rules. It offers an in-depth understanding that is crucial for a successful application process. Additionally, the document presents a thorough overview of the funding schema, outlining various opportunities and resources available to successful applicants. This approach aims to empower potential participants with the insights and knowledge needed to navigate the application process effectively and enhance their chances of receiving funding through the SECURED initiative.

1.1 Context

The SECURED project is launching an Open Call to drive the adoption and innovation of privacy-preserving technologies in healthcare. Aligned with the GDPR[1] and other relevant data protection regulations, SECURED focuses on developing tools that enhance secure data handling, anonymization, bias detection, synthetic data generation, and privacy-preserving computation. This Open Call seeks to empower Small and Medium Enterprises (SMEs), researchers, and healthcare innovators to integrate these advanced tools into real-world healthcare solutions. Through this Open Call, the SECURED project aims to extend its impact by supporting external innovators in applying privacy-enhancing technologies, and fostering collaboration within the European health data ecosystem. The initiative aims to facilitate real-world testing, expand the usage of SECURED technologies, and generate market potential by addressing critical privacy challenges in healthcare.

1.2 The SECURED Project

The SECURED project is a cutting-edge initiative that aims to advance secure multiparty computation (SMPC), homomorphic encryption (HE), data anonymization, and synthetic data generation. The project's main goal is to create a scalable, privacy-preserving framework that enables secure and unbiased artificial intelligence (AI) and data analytics, particularly within healthcare.

SECURED addresses current limitations in privacy technologies by improving algorithmic efficiency, enhancing the usability of privacy-preserving computation, and developing versatile tools that support a wide range of health applications. Key areas of focus include:

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation): https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679

- **Secure Multiparty Computation (SMPC)** and **Homomorphic Encryption (HE)** for health data analytics;
- Advanced methods for **data anonymization;**
- Tools for generating **synthetic health and medical data**, including images and datasets;
- A privacy-preserving federated learning infrastructure.

The project is anchored by four real-world healthcare use cases:

- Real-time tumor classification;
- Telemonitoring for children;
- Synthetic data generation for educational purposes;
- Access to genomic data.

The project takes on the challenge of overcoming existing limitations that hinder the widespread adoption of SMPC and effective anonymization. These challenges include practical limitations in current cryptographic schemes, the absence of standardized data anonymization methods for health data, and the lack of widespread methodologies for synthetic data generation. Additionally, the complex nature of federation protocols in machine learning and AI-based analytics poses obstacles, and there's a recognized need for supporting health technology providers in implementing privacy-enhancing technologies.

SECURED adopts a comprehensive approach to address these challenges. It focuses on scaling up privacy technologies through algorithmic improvements, enhancing hardware and software implementation efficiency, and generalizing primitives and definitions. The aim is to accelerate the development of privacy-preserving data-driven tools and services for a spectrum of healthcare applications, ranging from well-being and prevention to diagnosis, treatment, and follow-up care.

To ensure the practical relevance of its innovations, SECURED plans to showcase technologies developed through four health-related use cases. These use cases, in collaboration with partner hospitals and health stakeholders, encompass real-time applications that vividly demonstrate the efficacy and applicability of SECURED technologies in authentic healthcare settings. Beyond technological advancements, SECURED places significant importance on tackling ethical and legal challenges associated with data sharing.

The project strategically positions itself to encourage the adoption of developed technologies by providing direct support to relevant stakeholders through a dedicated funding call.

In essence, the SECURED project emerges as a pivotal force in overcoming current limitations in Data Privacy and Security. Through its multifaceted approach, including technological advancements, legal and ethical considerations, and dedicated support

for stakeholders, SECURED aspires to significantly contribute to the widespread adoption of privacy- preserving technologies in the landscape of healthcare.

By engaging external innovators through this Open Call, SECURED aims to expand the implementation of privacy-enhancing technologies, demonstrate their applicability in healthcare, and address legal and ethical challenges related to cross-border data usage.

2 SECURED Call for Proposals

The SECURED Open Call is designed to engage external stakeholders, including researchers, SMEs, and organizations in the healthcare sector, to test and validate privacy-preserving technologies. This section outlines the objectives, main characteristics, requirements, and funding scheme associated with the Open Call.

2.1 Objectives

The objectives of the SECURED Open Call are aligned with the broader goals of the SECURED project and focus on the following key areas:

1. **Validation of Solutions**: The Open Call aims to validate the effectiveness and applicability of the SECURED Innohub tools and services. External innovators, such as SMEs and researchers, are invited to create and implement actual health data analytics solutions using the SECURED framework. This validation process helps assess the real-world impact and viability of the developed solutions.
2. **Engagement of External Stakeholders:** The Open Call serves to engage external stakeholders, including professionals, practitioners, and academics from diverse backgrounds. By involving a broad audience, the SECURED project seeks to gather valuable insights, feedback, and perspectives on various aspects of the framework, ensuring a comprehensive evaluation.
3. **Raising Awareness and Momentum:** Through the Open Call, SECURED aims to raise awareness about its activities and solutions. By encouraging participation from a wide community, the project seeks to maintain a positive momentum, even beyond the completion of the SECURED project. This sustained interest is crucial for the long-term impact and adoption of SECURED technologies.
4. **Creation of Market Potential:** The Open Call is designed to create market potential for the SECURED project. By inviting external innovators to experiment with and adopt the SECURED tools, the project aims to foster a collaborative ecosystem and expand its reach within the health technology sector. This market potential contributes to the broader success and relevance of the SECURED initiative.

5. **Dissemination of Project Outcomes:** The Open Call facilitates the dissemination of project outcomes by broadening the testing environment of the SECURED solution. External innovators, through their participation, contribute to the dissemination of knowledge, refining the tools and propagating the generated insights. This dissemination is crucial for showcasing the impact of SECURED beyond the consortium.
6. **International Expansion:** Initially targeting European Union countries, the Open Call paves the way for international expansion, particularly in lucrative markets such as the United States. By inviting innovators from different regions, the project aims to establish a global presence and explore opportunities for cross-border cooperation.

2.2 Main Characteristics

The SECURED Open Call exhibits several key characteristics that distinguish it as a strategic initiative within the broader SECURED project.

Item	**Details**
Eligible Applicants	Small and Medium Enterprises (SMEs), researchers, health technology providers, academic institutions, and technology solution providers.
Open Call Time Frame	1 August 20244 - 31 October 2024 at 17:00 CET
Activities to be Funded	Development of health data analytics solutions using SECURED's framework, with a focus on privacy-enhancing technologies. These activities encompass real-world testing, integration, research, and innovation, with a specific emphasis on privacy-enhancing technologies.
Duration of Activities	Up to 5 months, divided in three stages: Planning, Implementation and Evaluation
Budget per Project	Up to €26,000 with an additional €1,500 for travel to the final event of the project. Each selected project is required to attend the final showcase meeting.
Evaluation of Proposals	Single stage. Evaluation by externals and consortium
Number of Proposals to be Selected	A minimum of **5 projects** will be funded
Milestones/payments	Stage 1 - Planning 30% Stage 2 - Implementation 40% Stage 3 -Evaluation and Reporting 30%

2.3 Proposal Requirements and Services

Applicants are required to submit proposals that comprehensively address SECURED's core objectives, specifically focusing on SMPC, data anonymization, synthetic data generation, and other privacy-enhancing technologies in healthcare. The SECURED framework will provide necessary tools and services for developing these solutions.

2.4 Funding Scheme

The SECURED Open Call has allocated a **total budget of €150,000** to support external third parties in developing privacy-preserving technologies within the healthcare sector. The funding will be used to validate, test, and expand the SECURED project's framework, particularly in the areas mentioned above.

- **Maximum funding per project**: €26,000
  Each selected project will receive up to €26,000 to cover costs related to the development, testing and implementation of privacy-enhancing technologies.
- **Travel costs**: €1,500
  In addition to the project funding, an additional €1,500 will be provided per project for travel expenses. This is specifically for physically attending the **final showcase Workshop**, where all selected projects will present their results. At least one representative of each project should be physically present to the final event.
- **Minimum number of selected projects**: At least 5 projects will be funded through this Open Call.
- A participant can only participate in one proposal only.

Funding will be distributed in the following stages:

1. **Stage 1 (Planning)**: 30% of the allocated budget will be released upon the completion and approval of the project's detailed planning phase;
2. **Stage 2 (Implementation)**: 40% of the budget will be provided after the successful execution of the primary implementation phase, including initial testing and integration of SECURED tools;
3. **Stage 3 (Evaluation and Reporting)**: The final 30% will be disbursed once the evaluation and reporting phase is complete, including the submission of a comprehensive project report outlining the outcomes and results of the project.

The funding process adheres to Horizon Europe's financial support to third parties, ensuring transparency, fairness, and alignment with the objectives of the SECURED project. All payments will be contingent on meeting predefined milestones and submitting the necessary documentation.

As aforementioned, , all selected projects are **required to attend and present their work** at the **final showcase Workshop**. This participation is considered an essential component of the final stage of the funding scheme.

2.5 Timeline

The following timeline outlines the key phases and deadlines for the SECURED Open Call.

Phase	**Date**
Call for Proposals Launch	1 August 2024
Proposal Submission Deadline	31 October 2024, 17:00 CET
Notification of Selected Projects	30 November 2024
Project Implementation Period	1 December 2024 – 1 May 2025
Completion of Project Work	1 May 2025
Final Showcase Event	**Note:** Exact date to be defined, will be after the end of all projects

Call Launch: The Open Call officially launched on 1 August 2024, allowing potential applicants to understand the requirements of the tender process, contact us for more details, and submit their proposals electronically.

Proposal Submission Deadline: All proposals must be submitted no later than 31 October 2024, 17:00 CET. Late submissions will not be accepted unless there are extenuating circumstances, which will be communicated via the SECURED website. All proposals are required to be submitted through the SECURED project website (https://secured-project.eu/).

Notification of Selected Projects: The evaluation process will conclude by 30 November 2024, at which point selected projects will be notified and invited to begin contract negotiations.

Project Implementation Period: The selected projects will begin on 1 December 2024 and are expected to complete their work by 1 May 2025.

Completion of Project Work: All project activities, including final reporting and deliverables, must be completed by 1 May 2025.

Final Event: Each funded project will be required to present its results at the final showcase Workshop, to be held after the end of all the projects. The exact date of the event will be communicated closer to the time.

Following the closure of the Open Call, the SECURED project will initiate the evaluation and selection phase, involving both external evaluators and members of the consortium committee. Internal evaluators will rigorously assess submitted proposals against the predefined eligibility criteria, and any proposal not meeting the criteria will be promptly notified and provided with a rejection letter. Eligible proposals will then proceed to the external evaluation phase, where external evaluators will review them. The top-ranked

proposals will receive notifications to enter the contract preparation and signature phase, while all other proposals, including those not meeting the threshold or placed on a reserve list, will be duly notified of their status. After the contract preparation is concluded, the projects begin their implementation phase, which is segmented into three stages:

1. Planning (1 month)
2. Implementation (3 months)
3. Evaluation and Reporting (1 month)

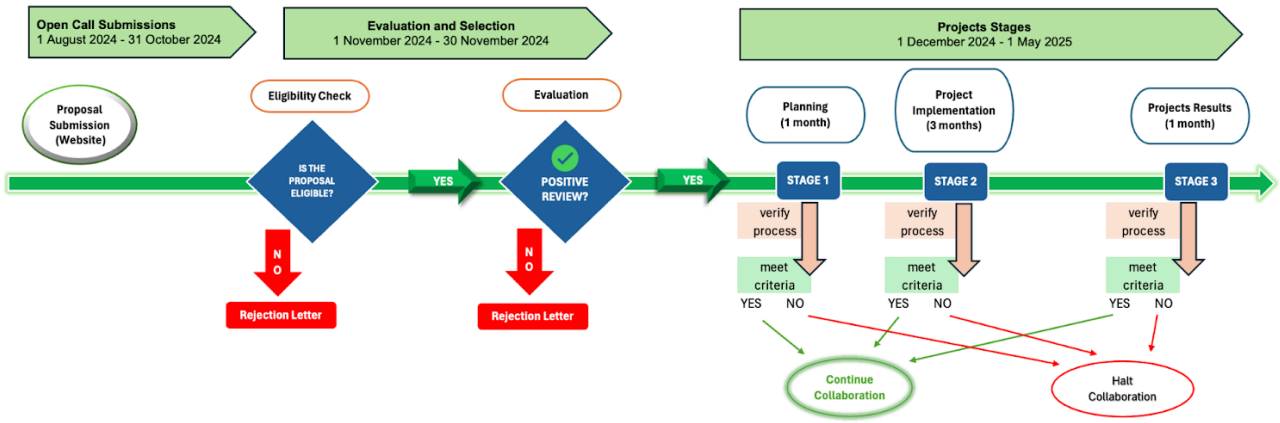

Figure 1. SECURED funding programme - Open Call

3 Eligibility Criteria

All applicants must adhere to the general requirements presented in this section to be considered eligible to participate in the SECURED- Open Call. The eligibility check will verify that:

- Submissions are made only through the SECURED website and by the defined deadline;
- Applicants are from an eligible Associated country;
- A participant can only participate in one proposal;
- Proposals and all requested documents are provided exclusively in the English language;
- The proposal description is submitted in accordance with the provided guidelines and template;
- A complete proposal is submitted, including the requested administrative data and any mandatory supporting documents specified in the Open Call (available through the application link);
- A proposal is only considered eligible if its content specifically aligns with the objectives of the SECURED Open Call, including the specific eligibility conditions set out in the relevant parts of the Guidelines of Applicants.

The eligibility check enables the establishment of a shortlist of proposals for evaluation.

To participate in the SECURED Open Call, applicants must meet the following eligibility criteria.

3.1 Applicants and Consortium Eligibility

- **Eligible Participants:** Participation is open to individuals, organizations, SMEs, academic institutions, research groups, and technology providers active in artificial intelligence (AI), machine learning (ML), data analytics, and healthcare.
- **Consortium Participation:** Single applicants or consortiums (collaborations of multiple entities) can apply. However, entities with conflicts of interest, such as SECURED consortium members, are not eligible.
- **Involvement of External Stakeholders:** The Open Call encourages partnerships with AI/ML experts, SMEs, healthcare providers, and research teams to test and validate privacy-enhancing technologies.

3.2 Eligible Countries

Only participants from countries eligible for Horizon Europe funding are allowed to apply. These include EU Member States and countries associated with Horizon Europe, as defined in the most recent version of the "EU Grants: List of Participating Countries[2]" document.

3.3 Proposal Eligibility

To be eligible for evaluation, proposals must:

- Be submitted before the **31 October 2024, 17:00 CET** deadline through the SECURED project website.
- Address the core objectives of the SECURED project, including privacy-preserving AI, secure multiparty computation, homomorphic encryption, advanced anonymization techniques, and synthetic data generation within healthcare.
- Include all required documentation and responses in English.
- Align with the legal, ethical, and technical frameworks set by SECURED.

3.4 Financial Eligibility

Funding Limits: The maximum funding per project is **€26,000** with an additional **€1,500** allocated for travel to the **Final Showcase Workshop**.

---

[2] List of Participating Countries in Horizon Europe: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/common/guidance/list-3rd-country-participation_horizon-euratom_en.pdf

All participants must provide the necessary financial documentation during the contract preparation phase, including VAT numbers where applicable. Failure to provide this may result in exclusion.

3.5 Language

English serves as the official language for the SECURED - Open Submissions. Any submissions in languages other than English will be deemed ineligible and will not undergo evaluation. Throughout the entire implementation of the SECURED funding program, English remains the sole official language. Consequently, all documentation and deliverables must be submitted in English to ensure eligibility.

3.6 Absence of Conflict

Applicants must not possess any existing or potential conflicts of interest with the SECURED selection process or throughout the entire project duration. Instances of conflict of interest will be individually evaluated.

Applicants are ineligible if they are partners or affiliated entities of the SECURED consortium, or if they are employees or collaborators under a contractual agreement with the consortium.

3.7 Documentation Format

Documentation for any phase must be submitted in **PDF format**, with no printing restrictions, in an electronic form.

4 Proposals - Process for Submission, Evaluation and Negotiation

4.1 Proposal Preparation and Submission

The submission process for the SECURED Open Call will adhere to the outlined steps in this section. Those intending to propose must be registered on the SECURED website (https://secured-project.eu/), which will serve as the central interface for proposal management during the Open Call.

The proposal submission process follows a streamlined procedure to ensure fairness, transparency, and compliance with the SECURED project's goals. The process is outlined as follows:

1. Registration and Proposal Submission: Applicants must register and submit their proposals (i.e.,Type of applicant, Applicant's name, Applicant's email, PIC number/ORCID id* (which applicable), Proposal's Title-Description and PDF File Proposals will only be accepted through this portal, and submissions by other means (email, post, etc.) will not be considered. The Open Call is open for

submissions from 1 August 2024 onwards, and the final submission deadline is 31 October 2024, 17:00 CET.

2. Proposal Components: Proposals must include a comprehensive project plan detailing how the applicant intends to use SECURED's tools and services to achieve the project's objectives. Proposals should specifically address one or more of the following areas: Secure SMPC, HE, Data Anonymization, Synthetic Data Generation, and Federated Learning.
3. Required documents include the **Application Form** and any supporting documentation specified on the SECURED website.
4. Proposals must be written in **English** and submitted in **PDF format**.

4.2 Submission Rules

Applicants are strongly encouraged to submit proposals ahead of the deadline to avoid any last-minute technical issues. The system-recorded time of submission will be final, and no extensions will be granted for late submissions unless there are widespread technical issues affecting the website.

4.3 Resubmission

Applicants may request to resubmit a corrected proposal if an error is identified before the deadline. However, the SECURED team cannot guarantee a timely response to such requests if they are made within 24 hours of the submission deadline.

Note: The system-recorded time of proposal receipt is definitive, and any delay in submission, regardless of the cause such as network delays or working from multiple browsers or windows, is not considered an acceptable extenuating circumstance.

4.4 Proposal Evaluation and Selection

The evaluation of proposals is carried out by the SECURED consortium with the support of independent experts. The SECURED consortium ensures that the process is fair and in line with the principles outlined in the European Commission's rules on proposal submission and evaluation. The collaboration with independent experts enhances the thoroughness and integrity of the evaluation process, aligning closely with the principles set forth by the European Commission for proposal submission and assessment. This concerted effort aims to guarantee a comprehensive and unbiased review, maintaining transparency and adhering to the highest standards outlined by the European Commission.

The evaluation process for the SECURED Open Call is designed to ensure a rigorous, transparent, and unbiased review of all submitted proposals. It will be conducted in two stages:

4.5 Eligibility Check (Stage 1)

The first step in the evaluation process involves thoroughly verifying the eligibility of proposals. The SECURED Open Call Management meticulously examines eligibility against predefined criteria. It is important to note that a proposal may be deemed ineligible or inadmissible at any point during this process. The verification entails:

- Ensuring that submissions are exclusively made through the SECURED website and within the specified deadline;
- Confirming that applicants are legal entities established in an eligible H2020 country, as outlined in section 3.2;
- Verifying that the proposal, and all required documents, is fully completed and presented solely in the English language;
- A proposal is considered eligible only if its content aligns with the objectives of the SECURED - Open Call, meeting specific eligibility conditions detailed in the relevant sections of the Guidelines for Applicants. This eligibility filter serves to create a shortlist of proposals for the subsequent stage of the evaluation process.

Proposals identified as non-eligible (for not meeting one or more eligibility criteria) will receive a rejection letter accompanied by a justification. It is important to note that no additional feedback on the process will be provided at this stage.

4.5.2 External Evaluation (Stage 2)

Proposals considered eligible will progress to the next stage (stage 2), will be evaluated by a panel of **experts**, chosen for their expertise in privacy-preserving AI, healthcare technologies, data analytics, and other relevant fields.

Each proposal will be evaluated based on the following key criteria:

- **Alignment with SECURED's Mission**: Does the proposal align with SECURED's goals of advancing privacy-preserving AI and data analytics, particularly in the healthcare sector?
- **Innovation**: Does the proposal introduce novel or creative approaches to solving privacy challenges in healthcare?
- **Feasibility**: Is the proposed project practical, and can it be realistically implemented within the given timeline and budget?
- **Impact**: Will the project significantly contribute to privacy-preserving AI in healthcare, and will it offer measurable benefits to the healthcare sector?
- **Resources**: Does the applicant or consortium have the required expertise and resources to successfully complete the project?

Each criterion will be scored from **0 to 5**:

- **0**: Fail (Criterion not addressed or missing).

- **1**: Poor (Serious weaknesses).
- **2**: Fair (Some weaknesses).
- **3**: Good (Addresses the criterion but with some room for improvement).
- **4**: Very Good (Strong with only minor areas for improvement).
- **5**: Excellent (Meets all requirements with no significant weaknesses).

Thresholds: To be considered for funding, a proposal must score at least **3 points** in each criterion. Proposals scoring below this threshold in any criterion or with an overall weighted average below **3** will be automatically rejected.

The score values will indicate the following assessments:

Score		**Description**
0	Fail	The Proposal fully fails to address the criterion under examination or cannot be judged due to missing or incomplete information.
1	Poor	The criterion is addressed in an inadequate manner, or there are serious inherent weaknesses that will impede success.
2	Fair	While the Proposal broadly addresses the criterion, there are significant weaknesses that would hinder the project implementation.
3	Good	The Proposal addresses the criterion well, although improvements would be necessary, and various details are missing on implementation.
4	Very Good	The Proposal addresses the criterion very well, although certain improvements are still possible, and some details are missing on implementation.
5	Excellent	The Proposal successfully addresses all relevant aspects of the criterion in question. Any shortcomings are minor.

The criterion threshold for each evaluation aspect is set at three (3). The overall score threshold, considering the final weighted average score, is also three (3). This means that any proposal scoring below 3 in any individual criterion or achieving an overall weighted score below 3 will result in automatic rejection. As the final score is calculated as a weighted average, it may include decimal values.

Each evaluator will document their individual assessment of each proposal through an Individual Evaluation Report. Subsequently, evaluators will convene for a consensus meeting to generate a unified Evaluation Summary Report (ESR) for each proposal. This summary reflects shared opinions and scores among evaluators, and it requires their signatures. A member of the SECURED Open Call Management will oversee and support this process.

It is essential to highlight that experts conduct evaluations independently and not as representatives of their employers, countries, or any other entities. Their role mandates independence, impartiality, and objectivity. All experts are obligated to sign a contract, including a declaration of confidentiality and the absence of a conflict of interest. Moreover, experts are bound by strict confidentiality throughout the evaluation process.

All proposed activities must adhere to fundamental ethical principles. Should any discrepancies related to these principles arise during the evaluation of the Proposal, the initiative will implement necessary measures to address the situation appropriately.

4.5.3 Ranking of proposals and Final selection

Upon completion of the evaluation process (Stage 2), all proposals will undergo ranking, resulting in a unified list. The primary criterion for ranking proposals will be their overall weighted average score, a comprehensive assessment incorporating criteria 1 to 5 with defined weights. Simultaneously, considerations will be given to the minimum and maximum number of proposals per service sub-category (refer to Table 2) to be selected. If there is an insufficient number of proposals for any service sub-category (either overall or those meeting the threshold), top-ranked proposals from other categories will be chosen.

In the event of proposals occupying the same position, tie-breaks will be resolved by giving precedence to those with the highest score in specific criteria, following this order:

Criterion 2: Impact
Criterion 1: Concept
Criterion 3: Feasibility/Implementation
Criterion 4: Consortium Composition
Criterion 5: Resource Allocation

After applying these tie-break rules, if proposals still share the same position, priority will be granted to those with a balanced representation of women and men in the consortium, aiming for a distribution closer to 50/50 in accordance with H2022 guidelines on gender equality.

The SECURED Open Call Management retains the right to arrange additional interviews with selected applicants to address queries regarding submitted proposals and provide further support in the evaluation process.

Selected projects will receive notification by **30 November 2024.**

4.5.4 Redress Procedure

If an applicant believes that the results of the eligibility checks have not been accurately applied or perceives a deficiency in the application of the SECURED - Open Call rules, they have the option to submit a request for redress. Requests for redress must:

- Be submitted within three (3) working days from receiving either (1) a rejection letter designating the proposal as non-eligible or (2) the ESR information letter.
- Specify the complaint's subject and provide a clear description, supported by arguments/evidence substantiating the objection.
- The complaint should be submitted by the legal representative of the entity that also submitted the proposal.
- Upon receiving a redress request, the SECURED Open Call Management will thoroughly examine the applicant's complaint. It will assess the complaint and propose an appropriate course of action. If there is evident proof of a deficiency that could impact the final funding decision, there is a possibility that some or all aspects of the proposal will be re-evaluated.

It's important to note:

- This procedure solely pertains to the eligibility/evaluation organizational process, without questioning the scientific or technical judgment of the expert evaluators involved in proposal evaluation.
- Re-evaluation will occur only if there is evidence of a deficiency influencing the final decision on funding the proposal.
- The evaluation score after any re-evaluation will be considered conclusive and it may be lower than the original score.
- Anonymous or incomplete complaints will not be taken into consideration.
- The SECURED Open Call Management will consider only one request for redress per proposal.

4.3 Sub-Protect Negotiation

4.3.1 Step 1: Contract Preparation and Negotiation

During the conclusion of the external evaluation phase, a minimum of 5 proposals will be chosen. All the not financed projects passing the accepting threshold will be added to the reserve list in the ranking achieved. This reserve list serves as a contingency in case a selected proposal fails to execute the sub-grantee agreement. Proposals assigned to the reserve list will be duly informed of this decision. All proposals will receive either an acceptance or rejection letter, accompanied by their respective evaluation reports.

The process of preparing the contract will undergo an administrative and financial examination, potentially extending to technical or ethical/security negotiations guided by

evaluators' feedback. Depending on the specifics of each sub-project's contract preparation, a telephone call or teleconference may be necessary and arranged to address any outstanding queries and provide clarification.

Once the evaluation process is completed, the top-ranked projects will enter the contract preparation phase. During this phase, the selected applicants will be required to submit additional administrative and financial documentation (e.g., VAT number, legal entity forms).

This phase may also involve technical and ethical clarifications as needed, based on feedback from evaluators. SECURED management may schedule calls or meetings to finalize any outstanding details.

Each participating entity should supply a valid VAT number during the contract preparation phase. Non-compliance with this requirement will lead to automatic exclusion from the contract preparation.

The SECURED consortium will communicate the request for the mentioned documentation to the sub-grant project representatives, specifying deadlines for the submission of information and documentation. If the necessary documentation and negotiations are not completed within the stipulated deadlines, the proposal will be automatically rejected, and the subsequent proposal in the reserve list will be invited to commence the contract preparation.

4.3.2 Step 2: Contract signature

Upon the conclusion of the contract preparation and negotiation phase, the sub-grant agreement (Annex 4) will be formally signed between the SECURED consortium, represented by the its the open call manager, Circular Economy Foundation (CEF), which also serves as the Treasurer, and the lead beneficiary acting on behalf of the contracting parties. This agreement outlines the contractual obligations and delineates the comprehensive work plan slated for implementation throughout the SECURED funding program. It signifies the formal commitment of the involved parties to the successful execution of the project.

4.3.3 Step 3: Reserve List

Proposals that meet the evaluation thresholds but do not receive immediate funding will be placed on a reserve list. This reserve list will serve as a contingency in case any of the initially selected projects withdraw or fail to meet the contract requireme

5 SECURED Funding Programme: Implementation, Technical Support, and Reporting

The SECURED funding program, corresponding to the open call, is designed to run for up to six months (Figure 1). This program is strategically organized into three distinct

stages, each meticulously crafted with specific objectives. As the project progresses through each stage, it is imperative for the sub-granted project to generate a comprehensive report detailing the outcomes and achievements of the work conducted during that phase. These progress reports serve as a crucial means of tracking and evaluating the project's advancements, ensuring transparency, accountability and alignment with the predefined objectives outlined in each stage. The robust reporting mechanism enhances the SECURED initiative's efficiency and facilitates continuous improvement throughout the program's duration.

The SECURED funding program is structured to ensure that selected projects are successfully implemented, closely monitored, and provided with the necessary support throughout the project lifecycle. The program is divided into three main phases: **Planning, Implementation,** and **Evaluation and Reporting**.

5.1 Implementation Phases

The project implementation is organized into three key phases:

1. Planning Phase (1 month):

Start Date: Projects begin on 1 December 2024.

Activities: In the first month, selected projects are required to finalize a detailed project plan, outlining the timeline, resources, and specific activities that will be carried out. This plan must align with the objectives outlined in the original proposal.

Deliverable: Submission of a comprehensive project plan, including milestones, a detailed budget breakdown, and risk assessment.

Funding: **30%** of the total project funding will be released after the successful completion of the Planning Phase, pending approval of the project plan.

2. Implementation Phase (3 months):

Activities: The core development and implementation of the proposed solutions will take place during this phase. Projects must focus on integrating the SECURED tools (e.g., secure multiparty computation, data anonymization, synthetic data generation) into their healthcare AI solutions, conducting initial tests, and refining the solutions based on feedback.

Mid-term Review: SECURED consortium members will conduct a mid-term review, which will assess the progress of each project and offer technical guidance if needed.

Deliverable: A mid-term progress report detailing the work completed, any challenges encountered, and adjustments made to the project plan.

Funding: **40%** of the total project funding will be disbursed upon successful completion of the mid-term review and approval of the progress report.

3. Evaluation and Reporting Phase (1 month):

Activities: In the final phase, projects are required to conduct a thorough evaluation of their results, measure the impact of their solutions, and document the outcomes. This phase also involves preparing the project's final report, which must include a comprehensive evaluation of how the objectives were met, challenges addressed, and lessons learned.

Final Presentation: All funded projects must present their results at the **final Showcase Workshop**, where they will showcase their innovations to the SECURED consortium, external evaluators, and relevant stakeholders in the healthcare and AI sectors.

Deliverable: A final report, including the project outcomes, technical evaluations, and documentation of the solution's impact on privacy-preserving AI in healthcare.

Funding: The remaining **30%** of the total project funding will be released upon submission and approval of the final report, along with participation in the final presentation at the Final Showcase Workshop.

5.2 Technical Support and Guidance

Throughout the duration of the SECURED funding program, selected projects will receive ongoing technical support and guidance to ensure smooth implementation and maximum impact. This support includes:

1. Access to SECURED Tools and Services:

Selected projects will have full access to the SECURED toolchain, which includes resources for secure multiparty computation (SMPC), homomorphic encryption, data anonymization, synthetic data generation, and federated learning infrastructure. SECURED will also provide templates, guides, and best practices for using these tools.

2. Expert Guidance:

Projects will benefit from technical consultations with members of the SECURED consortium. This includes one-on-one meetings with domain experts to help troubleshoot issues and refine the implementation process.

3. Workshops and Meetings:

At least **two meetings** will be organized between the SECURED consortium and selected projects. These meetings will focus on aligning project objectives, setting requirements, and presenting interim findings to receive feedback from consortium members and external evaluators.

5.3 Reporting Requirements

To ensure transparency and track progress, all funded projects are required to submit the following reports:

1. **Project Plan** (after the Planning Phase): A detailed plan outlining the scope of the project, milestones, expected results, and resource allocation.
2. **Mid-term Progress Report** (after the Implementation Phase): A report on the progress made during the implementation, including any modifications to the original plan, challenges faced, and solutions implemented.
3. **Final Report** (after the Evaluation and Reporting Phase): A comprehensive final report documenting the project outcomes, the impact of the solution on privacy-preserving AI in healthcare, and lessons learned. The final report must be submitted by **1 May 2025**.

Each report will be reviewed by the SECURED consortium. Any failure to submit these reports in a timely manner may result in delays or withholding of further funding.

5.4 Monitoring and Evaluation

The SECURED project management team will actively monitor the progress of each funded project to ensure that they adhere to the agreed timelines and objectives. This includes:

- **Periodic Check-ins**: Regular check-ins with project teams to ensure they are on track and to provide any necessary technical support.
- **Evaluation of Milestones**: The SECURED consortium will evaluate the achievement of milestones during each phase to ensure that the projects are progressing as planned.

6 Additional Information for Applicants

This section provides important details regarding the SECURED Open Call, including support resources, intellectual property rights, data protection and visibility requirements.

6.1 Support to Applicants

To assist applicants throughout the proposal preparation and submission process, the SECURED consortium provides the following resources:

1. **Frequently Asked Questions (FAQs):** A comprehensive FAQ document is available on the SECURED project website. This document addresses common questions related to eligibility, submission requirements, evaluation criteria, and funding procedures.
2. **Helpdesk Support:** Applicants can contact the SECURED helpdesk for any technical issues encountered during the submission process or for additional

clarification regarding the application guidelines. For inquiries, please contact: secured-open-call@list.uva.nl

3. **Templates and Documentation:** The SECURED project website offers templates for proposal submission, reporting and other necessary documentation. It is recommended to use these templates to ensure compliance with submission requirements.
4. **Submission Portal:** Proposals must be submitted through the dedicated submission portal on the SECURED website. The portal will guide applicants through each step of the process, and technical support will be available in case of any issues.

6.2 Intellectual Property Rights

Intellectual property (IP) rights related to the outcomes of the funded projects will be governed by the following principles:

Ownership: Applicants retain ownership of any intellectual property generated during the implementation of their projects. However, all participants are required to acknowledge the financial support of the SECURED project and the European Union (EU) in their outputs.

Access and Use: The SECURED consortium may request access to project outcomes (e.g., data, software, tools) for the purpose of further developing the SECURED toolchain and disseminating results. In such cases, appropriate agreements will be established to ensure the protection of applicants' IP rights.

Licensing: In cases where project outcomes include software or other tools, the applicants must ensure that they comply with the licensing terms set by the SECURED project. Open access or open-source licensing is encouraged but not mandatory.

6.3 Responsibilities of Beneficiaries

Selected applicants (beneficiaries) are expected to adhere to the following responsibilities:

1. **Compliance with Grant Conditions:** Beneficiaries must comply with all contractual obligations outlined in the sub-grant agreement, including financial reporting, technical reporting, and participation in scheduled events (e.g., the Final Showcase Workshop).
2. **Timely Reporting:** All required reports (planning, mid-term, and final reports) must be submitted according to the timeline specified in Section 5.3. Failure to submit reports on time may result in the suspension or termination of funding.
3. **Visibility and Acknowledgment of EU Funding:** Beneficiaries are required to promote the SECURED project and acknowledge the funding provided by the EU

in all project-related communications, presentations, and publications. The following statement should be included:
"This project has received funding from the European Union's Horizon Europe program under Grant Agreement No. 101095717."

4. **Participation in Events:** Beneficiaries must attend and present their results at the Final Showcase Workshop, as this is a critical part of the dissemination and validation process for the SECURED Open Call.

6.4 Conflict of Interest

Applicants must ensure that there is no conflict of interest that could impair the impartiality of the proposal evaluation or project implementation process. The following guidelines apply:

Declaration of Conflict: Applicants must declare any existing or potential conflicts of interest at the time of proposal submission. This includes any personal, financial, or organizational conflicts with members of the SECURED consortium or external evaluators.

Evaluation: The SECURED consortium will assess all conflicts of interest declared by applicants and take appropriate measures to address them. Proposals found to have unmanageable conflicts of interest may be disqualified.

6.5 Promoting the action and give visibility to the EU funding

As part of the requirements set forth by Horizon Europe, beneficiaries must ensure the visibility of EU funding in all project-related activities. This includes:

Acknowledgment of EU Support: All publications, presentations, and communications related to the project must include acknowledgment of EU funding, using the statement provided in Section 6.4.

Dissemination of Results: Beneficiaries are encouraged to share the results of their projects widely, contributing to the long-term impact of the SECURED project and the broader adoption of privacy-preserving AI technologies in healthcare.

Participation in Dissemination Activities: Beneficiaries may be invited to participate in additional dissemination activities organized by the SECURED consortium or the European Commission, contributing to the promotion of privacy-preserving healthcare technologies.

6.6 Data protection

Applicants and beneficiaries must ensure compliance with data protection regulations, including the GDPR. The following rules apply:

Data Handling: Any personal data processed during the project must comply with GDPR. Beneficiaries must ensure that data is processed lawfully, transparently, and securely.

Data Privacy in Project Outputs: Any tools, models, or services developed as part of the project must incorporate strong data privacy measures, aligning with the privacy-preserving objectives of the SECURED project.

Data Sharing: Beneficiaries must obtain the necessary consents and approvals for sharing any personal data collected during the project. Cross-border data sharing must comply with legal and ethical standards, and beneficiaries are responsible for ensuring this compliance.

7 Contact Information

For further inquiries regarding the SECURED Open Call, applicants can reach out through the following channels:

- Email: secured-open-call@list.uva.nl
- Website: https://secured-project.eu

Applicants are encouraged to check the SECURED website regularly for updates, additional guidelines, and relevant announcements regarding the Open Call.