



# SECURIT

TOWARDS RESILIENT SMART CITIES & TERRITORIES

## Guide for Applicants (GfA) SecurIT 1st Open Call for Applicants

Open date for proposals: 25 January 2022 at 13:00 CET (Brussels Time).

Deadline: 26 April 2022 at 17:00 CEST (Brussels Time).



## Table of content

1. Basic Info about SecurIT	3
2. What do we offer?	4
3. Eligibility Criteria	4
3.1 Who are we looking for?	5
3.2 What types of activities can be funded?	5
3.3 Ideal Project	7
3.4 How to apply?	9
4. How will we evaluate your proposal?	11
4.1 Step 1: First Automatic Eligibility Check	12
4.2 Step 2: Pre-scoring	12
4.3 Step 3: External Evaluation	13
4.4 Consensus Meeting	15
4.5 Jury Day	16
4.6. Ethical Review	17
4.6 What's next? Sub Grant Agreement and Signature	17
5. Our Support Programme and Payment Arrangements	18
6. Contact us	20
7. Last but not least - final provisions	21
8. Extra hints before you submitting your proposal	22
Annex 1: Information Clause	24
Annex 2: SecurIT Challenges and areas of needs	26

## 1. Basic Info about SecurIT

SecurIT (<https://securit-project.eu/>) is an EU-funded project aiming to create a new global competitive security industry (product & service) by supporting a better integration of innovative security systems.

This will be achieved by:

- supporting the **development and integration of innovative security solutions** in a new industrial value chain (and services);
- co-financing and supporting the **development of collaborative projects** allowing the **prototyping and experimentation** of technological solutions in the field of security, taking into account the ethical, legal and societal challenges of this sector;
- promoting **cross-border cooperation** between SMEs and other innovation actors in this sector.

**SecurIT** aims to focus on **increasing the security of current applications, services and infrastructures** by **integrating state-of-the-art security solutions or processes**, supporting the creation of lead markets & market incentives in Europe, following an end-user driven approach.

The SecurIT project is coordinated by [SAFE CLUSTER](#) and involves eight [partners](#) from six EU countries. The total SecurIT budget is € 4 958 031,25, out of which € 3.521.000 will be distributed to SMEs as financial support under 2 Open Calls, with a budget of € 1.760.500 per call.

This document summarizes the main points of the 1st Open Call for Applicants, under the SecurIT project, which will be **open from 25 January 2022 at 13:00 CET (Brussels Time) with a deadline on 26 April 2022 at 17:00 CEST (Brussels Time)**. The total budget of 1st SecurIT Open Call is € 1.760.500. The 2nd Open Call is scheduled for the beginning of 2023.

### Where can you find key information regarding this Open Call?

- [SecurIT](#) website for general information about the program,
- If you have any technical problems or doubt when filling in the online Application Form at FundingBox, tell us directly at [info.securit@fundingbox.com](mailto:info.securit@fundingbox.com)
- Application website <https://securit.fundingbox.com>

## 2. What do we offer?

Under 1st Open Call SecurIT will select up to **21 projects aiming to develop new prototypes or demonstrators in the security and cybersecurity domain** with financial and mentoring support from the SecurIT consortium. Projects must be submitted by consortia of at least 2 SMEs (at least one SME should be a technology provider) and must address one of the challenges described in Section 3.2.

SecurIT is offering **2 types of Instruments**:

- **Prototyping Instrument:** for the development of prototyping solutions for end-users or/and cybersecurity integrators at the MVP (Minimum Viable Product) stage at least. Under this instrument SecurIT will support you in translating your feasibility plan into a prototype,
- **Demonstration Instrument:** for new app solutions in cybersecurity and digital applications applying to security solutions ready to piloting at a large scale in the short-term. Under this instrument, SecurIT will support the piloting and validation of your solution in the relevant environment.

Selected consortia will enter up to 12-months Support Programme and receive:

- **Up to € 74.000** per 1 prototype project (maximum € 60.000 per SME),
- **Up to € 88.000** per 1 demonstration project (maximum € 60.000 per SME).

You (SME/consortium) can apply only to one of the instruments offered by SecurIT, based on the maturity of your solution.

The final number of projects selected per each instrument will depend on the overall quality of the proposals.

Apply here: <https://securit.fundingbox.com/apply>

## 3. Eligibility Criteria

We will check the eligibility of all proposals submitted before the deadline via our online application form (<https://securit.fundingbox.com/apply>). All the eligibility criteria are listed in this Section of this Guide for Applicants.

The projects that do not comply with those criteria will be excluded and marked as ineligible. We will check the eligibility criteria based on the information provided in your application during the whole evaluation process.

## 3.1 Who are we looking for?

We are looking for consortia of at least 2 SMEs<sup>1</sup> [registered legal person] established in:

- The Member States of the European Union and its Overseas Countries and Territories (OCT) or
- [Associated Countries to H2020](#)<sup>2</sup>

At least one SME in the consortium should be a **technology/IT solution provider**.

All SMEs applying as one consortium should be autonomous to one another (without capital or personal links).

The SecurIT partners or their affiliates or employees, are NOT considered as eligible applicants and can NOT apply for funding.

## 3.2 What types of activities can be funded?

SecurIT is looking for projects that address the development and implementation of technology and systems related to the specific challenges (listed below) defined in collaboration with end-users and integrators.

Depending on the maturity of your solution, you can choose between 2 different types of Instruments offered by SecurIT:

- if you are interested in **building the prototype/MVP** of the solution: apply to **Prototyping Instrument**,
- if you already have a prototype/MVP and would like to **pilot** them: apply to **Demonstration Instrument**.

### **What are the challenges to be addressed by SMEs?**

The challenges have been defined around 3 main domains:

---

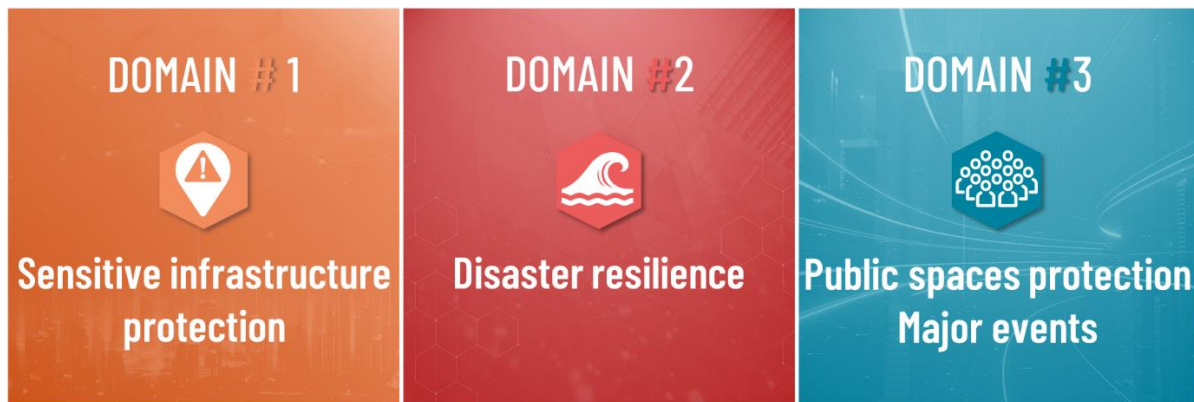
<sup>1</sup> An **SME** will be considered as such if it complies with the European Commission's Recommendation 2003/361/EC. As a summary, the criteria defining an SME are:

- Headcount in Annual Work Unit (AWU) less than 250;
- Annual turnover less or equal to €50 million OR annual balance sheet total less or equal to €43 million.

Note that the figures of partners and linked enterprises should also be considered as stated in the SME user guide. For detailed information check EU recommendation:

[https://ec.europa.eu/growth/smes/business-friendly-environment/sme-definition\\_en](https://ec.europa.eu/growth/smes/business-friendly-environment/sme-definition_en)

<sup>2</sup> For UK applicants: the UK is an EU associated country, due to this the UK applicants are eligible at the time of the deadline of the open call



- **Domain #1: sensitive infrastructure protection**

Sensitive infrastructure protection pertains to the securing of assets and systems that are essential for the functioning of a society and economy. Examples include the provision of gas and oil, agriculture, and telecommunication. The security of sensitive infrastructure is a major concern, confirmed by recent events, in the context of social unrest, terrorist threats and even a pandemic. If this type of infrastructure is exposed to external threats, this will have major consequences for society as a whole.

Targeted end-users: for example, end-users of projects around sensitive infrastructure protection include the safety director of vital importance and Seveso classified industrial facilities, airports, hospital infrastructure, and operators (e.g. electricity, gas, telecommunications, etc.)

Solutions: The solutions developed in this domain will have to integrate the following considerations: maintainability, acceptable price, foresight scanning, and interoperability with existing solutions.



CHALLENGES and potential areas of needs:

1. Development of cybersecurity solutions for sensitive infrastructure protection
2. Optimisation of communication networks and alert systems
3. Development and optimization of identification and access control for rapid access in the site, all while ensuring that no one and nothing that enters poses a security risk.
4. Development of solutions to detect and locate any intruders that have managed to penetrate the perimeter protection and barriers to block intrusions

- **Domain #2 - Disaster resilience**

There is a need for instruments that facilitate improved prevention and preparedness in crises and natural disasters. The development of technologies for first and second responders, and where relevant for citizens, that increase societal resilience is the second focus-area of the SecurIT project. Innovative technologies can help detect, analyse, treat, and/or prevent major natural events. This domain focuses mainly on climate-

related risks and extreme events, geological disasters such as wildfires, earthquakes, tsunamis, and pandemics.

Targeted end-users: for example, first responders, cities and territories, and their governmental structures.

Solutions: The solutions developed in this domain will have to consider citizen involvement and acceptance and transparency. All solutions will also have to ensure the continuity of operations.



#### CHALLENGES and potential areas of needs:

5. Optimisation of prediction of disaster
6. Optimisation of communication and warning systems in case of disaster
7. Development of solutions for a better recovery

- **Domain #3 – Protection of public spaces**

The objective of this domain is to develop innovative tools that create increasingly connected and protected cities in which the population takes on a more active role in serving the community. These solutions should integrate and consider state-of-the-art technologies like in Artificial Intelligence, Cloud computing, and Big Data.

Targeted end-users: for example, cities and territories (security of public roads), and venues open to the public (e.g.: stadiums; concert zone, train stations, etc.).

Solutions: The solutions developed in this domain will have to consider the legal constraints of personal data protection.



#### CHALLENGES and potential areas of needs:

8. Gather and manage real time information
9. Analyse and extract pertinent and potentially crucial information as quickly as possible
10. Communication networks and post -event analysis
11. Detection

The challenges listed above can be broadly interpreted/are non-exhaustive. Detailed description of each challenge is included in the Annex 2.

### 3.3 Ideal Project

The ideal project is a use case of prototyping or demonstration of the security solution that addresses at least one of the challenges in the following areas:

- cybersecurity,

- digital applications applying to security solutions.

The demonstrators that will be implemented should be tested in operational environments. The demonstrations can be considered very near to market exploitation.

For Prototyping Instrument it is expected that the initial TRL (**Technology Readiness Level**<sup>3</sup>) is a minimum of 5 while the TRL reached by the end of the project will be a minimum TRL 6/7.

For Demonstration Instrument it is expected that the initial TRL is minimum 5 while the TRL at the end of the project is minimum TRL 8/9.

The ideal applicant is a consortium composed of 2 (two) SMEs from different eligible countries, however, we also accept consortia of SMEs registered in the same country. Please be aware that international consortia will get a bonus in the scoring process (1 extra point).

At least one SME must be a **technology/IT solution provider**. It's also recommended that at least one consortium member has **experience in the domain or sector** that the consortium is applying to.

### *Ideal Project Examples*

*Example 1 (challenge to solve: identification and access control of domain):*

*A consortium of 2 SMEs from Austria and Spain proposes a digital system that permits access control with an intelligent badge system for authorized persons in charge of protection of critical or sensitive venues. The consortium applies to the demonstrator instrument, in order to test in a near-real environment their solution, addressing challenge 3 - identification and access control. They are assisted for this by the safety director of an industrial SEVESO site that will provide the field for experimentation and testing of the solution.*

*Example 2 (challenge to solve: Prior to crisis – prediction/Risk knowledge and evaluation)*

*1 SME from the Netherlands and 1 SME from Bulgaria gather into a consortium to develop tools to map the vulnerability of the territory, i.e. the conjunction between natural disaster potentiality and human capability to face the event. The product they develop here goes beyond the state of the art, uses AI and integrates aerial imagery and past event consequences analysis or a societal filtered analysis.*

---

<sup>3</sup> TRL, Technology Readiness Level. Technology Readiness Levels (TRLs) are indicators of the maturity level of particular technologies. This measurement system provides a common understanding of technology status and addresses the entire innovation chain. There are nine technology readiness levels; TRL 1 being the lowest and TRL 9 the highest. In our project, we refer to [Annex G of the General Annexes](#) to the Work Programme 2016/17 for a full description of TRLs.



### Example 3 (challenge to solve: Detection of alert)

An SME provider of AI solution from Italy and a small company from Sweden, specialized in analysing human behaviour are developing a prototype of an intelligent flow management system, that could detect suspicious and abnormal behaviour. Their innovative solution is selected in SecurIT open call to participate in the support program and receive a FSTP grant of € 74.000 for delivering the MVP. AI solution provider will receive € 50.000 and its consortium partner from Sweden will get € 24.000 during the 12-month program.

## 3.4 How to apply?

Applying to an open call takes time and dedication and we are grateful you take up the challenge of applying to the SecurIT Open Call. Because we care, we simplified the process as much as possible and we would like to make sure you understand what are some of the eligibility requirements with which you have to comply to.

- **Have a European dimension:** your proposal should have a clear European dimension meaning that the challenge is to fully exploit the potential of the European economy and society. Building notably on Europe's Scientific and Technology strengths in the field. The supported activities should reinforce industrial competitiveness across security solutions. The ambition is to bring development and integration of innovative security solutions in a new industrial value chain (and services).
- **Submit in time:** Make sure you submit your proposal through the online form dedicated to the right type of Instrument: <https://securit.fundingbox.com> before the **deadline** (Deadline: 26 April 2022, 17:00 CEST). If you submit the form correctly, the system will send you a confirmation of your submission. Get in touch with us if it is not the case. It is important for you to know that we will not be evaluating any proposal sent after the deadline and submitted outside the dedicated form.
- **Be exhaustive:** Have you answered all the sections of the form? It won't be possible to add any information after the deadline. However, you will be able to modify the form as much as you like even *after* the proposal is submitted, **as long as it is done before the deadline**.
- **Less is more:** You can apply to only one type of Instrument and submit **only 1 proposal** (as a single SME and as a consortium). If more than one proposal is submitted by you, your consortium or your consortium partner (taking into account all applications submitted in both Instruments), only the last edited proposal which has been submitted will be evaluated. Other proposals will not be eligible. So no point multiplying your chances this way, it is better to submit only one proposal and make it shine.

- Your proposal must be written in **English** in all mandatory parts in order to be eligible. Only parts written in English will be evaluated.
- **Every question deserves your attention:** all mandatory sections of your proposal - generally marked with an asterisk - must be filled in. Make sure that the data provided is true and complete. This is crucial for us to properly assess your proposal. Conversely, any additional material that is not specifically requested in the online application form will not be considered for the evaluation so no point overdoing it.
- **Conflicts of interest:** we will take into consideration the existence of the potential **conflict of interest** between you and one or more SecurIT Consortium partners. Indeed, consortium partners, their affiliated entities, employees and permanent collaborators cannot take part in the SecurIT programme. Although, being a member of an association participating in the execution of the SecurIT programme does not mean that you are not allowed to submit an application. All cases of potential conflict of interest will be assessed case by case.
- **Healthy finances and a clean sheet are a must:** we won't accept entities that are under liquidation or enterprises in difficulty according to the Commission Regulation No 651/2014, art. 2.18. Neither will we accept proposals from entities that are excluded from the possibility of obtaining EU funding under the provisions of both national and EU law, or by a decision of both national or EU authority.
- **It is your proposal:** your project should be based on your original work. If not, that's okay, just make sure your right to use the IPR is 100% certain. Going forward, any foreseen developments must be free from third-party rights and if not, these third-party rights must be clearly stated.

SecurIT planned a certain number of online webinars about this open call. They will be announced at the SecurIT website. You are also welcome to reach out to the project partners for more information.

#### Eligibility criteria checkpoint:

- You are applying as a consortium of at least 2 SMEs from eligible countries, at least 1 of consortium member is IT/technology provider,
- You are addressing at least one of the SecurIT challenges, and choosing one of two instruments (Prototyping or Demonstration Instrument) at appropriate TRL level,
- You are submitting only 1 proposal (as single SME and as consortium), which has a clear European dimension and certain IPR rights,
- Your proposal is in English and all mandatory sections are filled in,
- You are using the online application form and submit your application before the deadline,

- You and your consortium member(s) are not under liquidation or in financial difficulty,
- You and your consortium member(s) are not excluded from the possibility of obtaining EU funding,
- You and your consortium member(s) do not have a conflict of interest with any of SecurIT Consortium partners.

## 4. How will we evaluate your proposal?

Our evaluation process is transparent, fair and equal to all our participants.

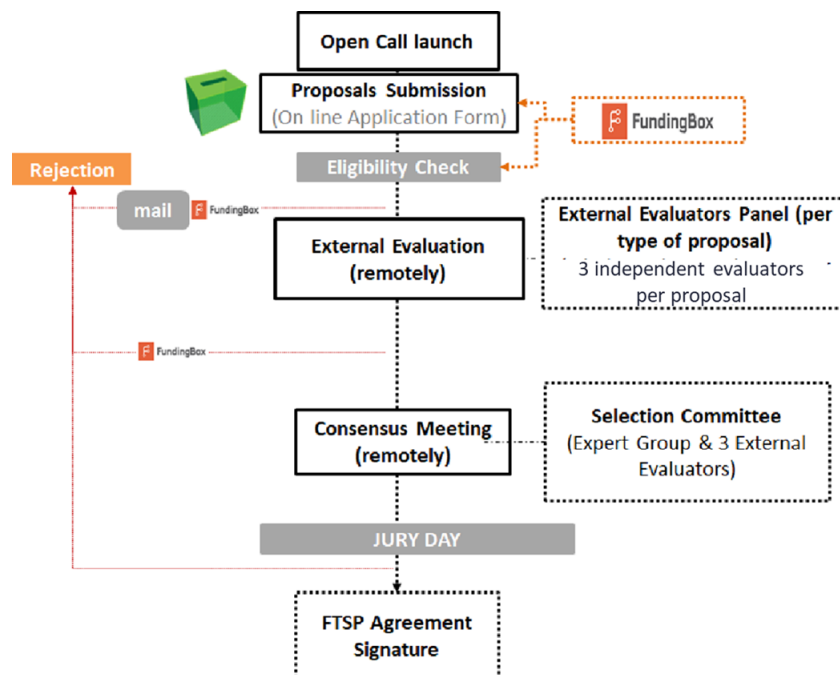


FIGURE 1. SELECTION PROCEDURE

We will be evaluating your project in 5 phases. The evaluation process of applications submitted to each Instrument will be done separately (it means that your application will be competing only with applications submitted to the same Instrument).

We expect a high number of applications so if you want to stand out, quality is the way to go. What does it mean? In short, provide as many details as possible while being extremely clear and structured.

This will help us to identify properly the key points of your application and see how it fits within the overall SecurIT scope.

## 4.1 Step 1: First Automatic Eligibility Check

The first evaluation step is about verifying some basic requirements based on the statements from your proposal. Your proposal will be admissible for the next phase if it:

- Is **complete, readable and in English** in all mandatory sections.
- Has been submitted via the online form <https://securit.fundingbox.com> within the **deadline** (26 April 2022, 17:00 CEST). You won't be multiplying your chances by applying several times, it is only the last application that you edited (after submission) that we will be evaluating in case there is more than one application that you are part of.
- Includes the properly filled declaration of honour. Read carefully the **Declaration of Honour** template included in the application form [here](#), as we will check the related submitted statements. You will not be able to change them after the deadline.

Moreover, a first check regarding the eligibility of the participants specified in section 3 will be carried out.

Following this first step, we will move on to the pre-scoring phase described below.

## 4.2 Step 2: Pre-scoring

If we receive more than 60 eligible proposals (in total for both Instruments), a pre-scoring system may be included to help us make a pre-selection.

What does this mean? The FundingBox Open Call Management System (FundingBox Enterprise) will automatically assign a score to the eligible proposals according to the following criteria:

- Dedication to the project (consortium as a whole) (13% weight / up to 13 points)
- Team skills (14% weight / up to 14 points)
- Proved experience in the target market (15% weight / up to 15 points)
- Scalability of the solution (13% weight / up to 13 points)
- Market opportunity (10% weight / up to 10 points)
- Status at technological level (10% weight / up to 10 points)
- Human resources for developing security solution (10% weight / up to 10 points)
- Consortium composition at the geographical level (15% weight / up to 15 points)

As an applicant, you should:

- select the option that best describes the characteristics of your project in relation to each criterion,

- confirm that no false declarations are made.

In total, your project can receive up to **100 points**. If your score places you in the best-marked applications (up to **60 top-ranked** applications will be selected in total), well done! As a next step, we will forward your application to an external pool of experts for a more detailed and qualitative evaluation and scoring.

We will inform you about the results of the eligibility check and the pre-scoring phase soon after these steps have been completed, generally in 2 weeks that follow the deadline to submit the application.

### 4.3 Step 3: External Evaluation

You have reached the external evaluation phase: bravo! And if not, be persistent: there may be other open calls for this project and other funding opportunities may suit - even better - your proposal.

**For those who have been selected:** from now on, each project will be evaluated by **3 external and independent** evaluators appointed according to the specific characteristics of your project.

These are criteria they will consider to complete the evaluation:

**(1). EXCELLENCE** will evaluate:

- **Ambition.** The applicants have to demonstrate to what extent that proposed project is beyond the State of the Art and describe the innovative approach behind it (e.g. ground-breaking objectives, novel concepts and approaches, new products, services or business and organisational models).
- **Innovation:** applicants should provide information about the level of innovation within their market and about the degree of differentiation that this project will bring.

**(2). IMPACT** will analyse:

- **Market opportunity:** The applicants have to demonstrate a clear idea of what they want to do and whether the new/improved product/service has market potential, e.g. because it solves a problem for a specific target customer.
- **Competition:** The applicants have to provide information about the degree of competition for their particular product/service and if the idea is disruptive and breaks the market. i.e. the products/services to be brought to market can be clearly differentiated from the competition.
- **Commercial Strategy and Scalability:** The applicants have to demonstrate the level of scalability of the new/improved product/service, meaning that it doesn't address the solution of a specific problem but it's able to be commercialised to solve a structural problem in a specific sector/process/etc.

(3). IMPLEMENTATION will consider:

- **Team:** The applicants have to demonstrate their management and leadership qualities, their ability to take a concept from ideas to market, their capacity to carry through their ideas and understand the dynamics of the market they are trying to tap into as well as their technical capabilities to reach the defined objectives. The team should be a balanced and cross-functional team, with a strong background and skill base.
- **Resources.** Demonstrate the quality and effectiveness of the resources assigned in order to get the objectives/deliverables proposed.
- **Risk management:** the applicants have to present the risk assessment and propose measures to overcome them, especially the applicant should provide information about the legal constraints related to the project execution.

**Transversal criteria** such as ‘Environment and low carbon economy contribution’, ‘Equal Opportunities including Gender Balance’ and ‘Social Impact’ will be also considered by evaluators when scoring the proposals.

The evaluators will score each criterion on a scale from 0 to 5:

0 = The proposal fails to address the criterion or it cannot be assessed due to missing or incomplete information.

1 = Poor – The criterion is inadequately addressed or there are serious inherent weaknesses.

2 = Fair – The proposal broadly addresses the criterion, but there are significant weaknesses.

3 = Good – The proposal addresses the criterion well but there are a certain number of shortcomings.

4 = Very good – There is a small number of shortcomings but overall, the proposal addresses the criterion very well.

5 = Excellent – The proposal successfully addresses all relevant aspects of the criterion with no or minor shortcomings.

Each evaluator will produce an **Individual Evaluation Report**. The final score will be calculated as an average of the individual assessments provided by the Evaluators.

Each criterion will be scored out of 5 points. The threshold for individual criteria will be 3 points. The overall threshold, applying to the sum of the three individual scores, will be 10 points.

In the case of ties, the following criteria will be used to rank the projects, in order:

- Transversal Criteria,
- Impact score,

- Implementation score,
- Excellence score.

All proposals obtaining a score above the threshold will move on to the next stage.

In addition, applications submitted by SME **applicants registered in 2 different eligible countries will be given 1 extra point** to the overall score.

After the external evaluation process 2 types of 'Ranking Lists' will be defined:

- the 'General Ranking List' where all the applications will be ranked according to their scores,
- the 'Ranking List of Projects per Instrument' for each type of funding instrument (2 lists in total).

Do note that the evaluation phase takes time as it implies a more personal, qualitative and thus non-automated approach. But eventually, your patience will be rewarded!

## 4.4 Consensus Meeting

Following the external evaluation, a 'Selection Committee' formed by selected consortium partners and, at least, three external experts, selected from a pool of experts that evaluated individually the proposals, will decide by consensus (minimum  $\frac{2}{3}$  of the votes), and based on the Ranking Lists per Instrument gotten as a result of the External Evaluation, the 'List of finalists' per each Instrument (**up to 31 projects in total**) to pass to the next phase.

Although the goal of SecurIT is to select indicatively 10 projects per Prototyping Instrument and 21 projects per Demonstration Instrument, the exact number of proposals selected per each Instrument might be different and will be decided based on the overall quality of the proposals included on each ranking list.

Bear in mind that even if it is normally the best-marked proposals that are selected for funding, the Selection Committee may have fair reasons for objecting to the selection of a specific candidate. These reasons can relate to:

- The alignment with SecurIT goals and scope.
- The ability to achieve the strongest possible impact.
- The low level of innovation.
- The existence of significant ethical concerns.
- The existence of a potential conflict of interest<sup>4</sup>.

---

<sup>4</sup> Please note that this is not a closed list of reasons for objecting

In case a top-ranked application is rejected, we will consider selecting the next best-ranked proposal.

## 4.5 Jury Day

If your proposal has been selected following the Consensus Meeting, well done!

You will be invited to on-site Jury Day (please be aware that in case the physical meeting will not be possible, Jury Day will be organized online), participation of at least one consortium member will be mandatory. It's recommended that both consortium members will be present at the Jury Day.

We will sign with your consortium a Mini-Grant Agreement of €1.000 for Jury Day as lump-sum. Each consortium will get €1.000 in total. It can be used for travel or other purposes related to the project such as the preparation of a video presentation.

Each consortium invited to Jury Day will be requested some basic legal information to confirm that the legal entities engaged in the proposal exist and to prepare the Mini-Grant Agreement which will be signed with selected consortia before the Jury Day event (one Mini-Grant Agreement per consortium). A mini-grant will be paid against attendance validation and signature of the Mini-Grant Agreement with the SecurIT Consortium.

During the Jury Day, you will have the opportunity to pitch your project in front of the SecurIT JURY composed of the Selection Committee Members and supported by Ethical Committee member(s).

Before Jury Day your consortium will be requested to submit a 5-minute video pitch, which will be reviewed by the Selection Committee, independently, before the Jury Day. The Selection Committee will agree on the Q&A for each applicant team, in order to make the session more efficient.

Sending a video pitch and attending the Jury Day by at least one consortium member are mandatory requirements; not attending any of these requirements will automatically imply the exclusion of the proposal from the list.

After the Jury Day, the SecurIT Selection Committee will undertake the **final evaluation** taking into account the following criteria:

- Quality of the team
- Innovative step in solving the challenge
- Feasibility of the project implementation
- Transversal criteria (final criteria in case of ties).



The Selection Committee will decide by majority votes ( $\frac{2}{3}$  from all members) on the “**Provisional Lists of recipients per Instrument**” as well as the ‘**Reserve Lists per Instrument**’.

**Up to 21 proposals in total** will be selected. The goal is to select 7 projects for Prototyping Instrument and 14 projects for Demonstration Instrument, however, the exact number of proposals approved per each Instrument might be different, depending on the overall quality of all proposals invited to the Jury Day. After the Jury Day, we will communicate the results.

## 4.6. Ethical Review

All the selected projects shall comply with ethical principles and relevant national, EU and international legislation. To ensure that each project is compliant with it, all selected projects will undergo an initial Ethics Review before signing the **Sub Grant Agreement**. The ethical implications of projects are assessed at the proposal evaluation stage, particularly with regard to:

- The use of data that is potentially traceable to a person,
- The use of, or interaction with, vulnerable individuals and groups,
- Potential physical or mental harm to operators, users and / or third parties,
- The development of systems liable to maintain or amplify societal disadvantage or discrimination based on race, gender, sexuality, social class or economic standing.

Where potential issues are identified, the applicants will be required to detail any mitigating actions which will be included in the ‘Ethics Summary Report’, and an Ethical Committee will be established to supervise and monitor the ethical concerns during the bottom-up project’s implementation.

## 4.6 What’s next? Sub Grant Agreement and Signature

You made it! You are part of the **final 21 selected** for the SecurIT open call. It has been a long journey. Or has it actually just started?

In any case, before you get started with SecurIT programme, you need to sign the Sub Grant Agreement with the SecurIT Consortium (for the details please check our Frequently Asked Questions Document).

Before signing the Sub Grant Agreement, you should provide documents regarding your formal and financial status. The SecurIT Consortium will proceed to a **verification of these documents** to make sure you are eligible.

**Be extremely vigilant with respect to:**

1. **The nature of the documents** we request. If the documents you provide us with do not prove your eligibility, the adventure will end here.
2. **The deadlines** that we will give you to hand us these documents. If you do not deliver the requested documents on time, without a clear and reasonable justification, we will have to exclude you from the further formal assessment. Another applicant from the Reserve list will then replace you.

## 5. Our Support Programme and Payment Arrangements

Once your eligibility has been confirmed following the formal check and the Sub Grant Agreement signed, you would be an official beneficiary of the SecurIT Programme. It is now that the adventure begins and it is now high time to understand how the funding is going to be distributed.

### Support Programme

The Support Programme will last up to 12 months. During this period you will be supported by the Experts from Top Security Clusters for bringing new technologies for security applications. We will support you in the prototype development or demonstrations (depending on the Instrument you selected) in the real condition in security domains.

As a beneficiary, you will receive a **fixed lump sum of:**

- **Up to €74.000 per project** (with a maximum up to €60.000 per SME under Prototyping Instrument, including Jury Day mini-grant),
- **Up to €88.000 per project** (with a maximum up to €60.000 per SME under Demonstration Instrument, including Jury Day mini-grant).

It's up to selected SMEs to agree on how the fixed lump sum will be distributed among SMEs under funded project (but no more than 60k per entity).

The lump sum is a simplified method of settling expenses in projects financed with Horizon 2020 funds. It means that you are not required to present accounting documents to prove the investment-related costs incurred (e.g. invoices). However, you are obliged to demonstrate that the implementation of the project is in line with the milestones set for it.

It is necessary to provide an explanation in the application on how the lump sum will be used to reach the defined objectives but detailed reporting of the spending, cost statements and time sheets are not requested after the end of the project. Since the granting of a lump-sum doesn't foresee the delivering of a cost

statement, the use of the project budget will be controlled considering the technical advancements by the SecurIT experts.

The application form must include information how the grant will be distributed between consortium members. When preparing your budget split, please remember that it is strongly recommended that subcontracting is limited to a maximum 30% of the lump sum.

The milestones (deliverables, KPIs and ethical recommendations) will be defined and calendarised in the '**Follow Up Plan**' elaborated at the beginning of the programme with the support of the *Follow up Manager* assigned to guide through the whole Support Programme.

In short, we will carefully assess your progress and the quality of your work during Interim Reviews but we will not review your accountancy.

Bear in mind that the lump sum does not release you from the obligation to collect documentation to confirm the costs under fiscal regulation.

The *Follow Up Plan* will become an Annex to Sub Grant Agreement and establishes the budget planned for execution of your projects, KPIs and Deliverables that will be taken into account when evaluating your project's performance during Interim Reviews at M6 (Interim Report) and M12 (Final Report).

The payments will be done once the deliverables are approved by the 'Mentoring Committee' and validated by the 'Selection Committee'.

The corresponding evaluation criteria is as follows:

- Deliverables quality (based on the Deliverables established in the *Follow Up Plan*).
- Technical performance indicators (based on the KPIs established in the *Follow Up Plan*).
- Deadline Compliance.

Each criterion will be scored from 0 to 10 and the weight of each one of these criteria, in the final score, will be as follow:

- Deliverable quality (45%).
- Technical performance indicators (45%).
- Deadline Compliance (10%).

According with this final score:

- Beneficiaries over the threshold (7 points) will successfully receive the next payment and continue in the program.

• Beneficiaries under the threshold will be reviewed by the ‘Selection Committee’ who will take the final decision taking into account all possible objective reasons for underperformance (i.e. external factors which might have influenced the beneficiaries’ performance).

Those not passing this examination will not receive the next payment and will be invited to leave the Program.

The beneficiaries will receive the funding as follows:

- 1st instalment: up to 20% of maximum grant amount (at M1 after validation of the *Follow Up Plan*),
- 2nd instalment: up to 80% of maximum grant amount (at the end of the support program, after validation of the MVP or Pilot).

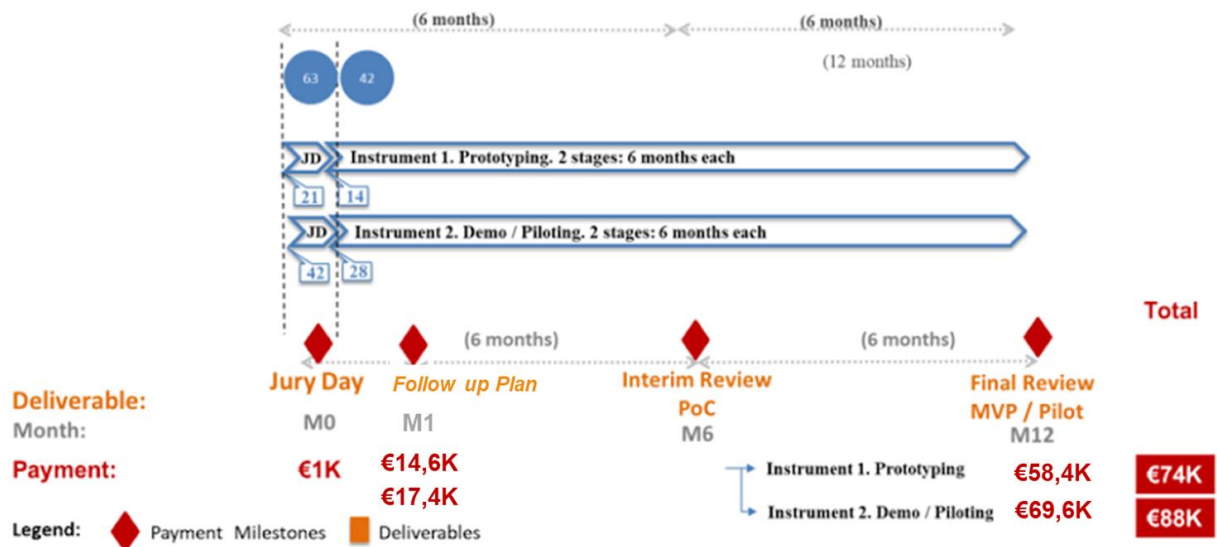


FIGURE 2 SUMMARY OF THE SUPPORT PROGRAM AND MAXIMUM AMOUNTS OF GRANTS PER EACH STAGE

Lastly, for a more detailed payment schedule, you can read our [Frequently Asked Questions](#).

## 6. Contact us

If you still have any doubts regarding our Open Call process, feel free to get in touch with us and send us an email to the following address: [info.securit@fundingbox.com](mailto:info.securit@fundingbox.com).

If ever you face any technical issues or problems, make sure you include the following information in your message:

- Your username, telephone number and your email address.
- The details of the specific problem (error messages that appeared, bug descriptions such as a dropdown list that isn't working, etc.).
- Screenshots of the problem.

## Complaints

First of all, be aware that we won't be reviewing your complaint **if**:

- ...It is anonymous.
- ...The information is incomplete.
- ...It is not related to the results of the evaluation phases. Indeed, most of the evaluation process is run by **independent experts** in the given field. The project consortium does not interfere with their assessment.

If, after receiving the results of the one of the evaluation phases, you consider that a mistake has been made, resulting in the rejection of your application, you have the right to send us a complaint. You can email us in English to: [info.securit@fundingbox.com](mailto:info.securit@fundingbox.com) including the following information:

- Your contact details (including email address).
- The subject of the complaint.
- Information and evidence regarding the alleged mistake.

### **Important note regarding the timeline:**

You have **3 calendar days** to submit your complaint starting from the day after the communication was sent. On our side, we will review them within no more than **7 calendar days** from its reception. If we need more time to assess your complaint, we will inform you by email about the extension.

We will not review anonymous complaints as well as complaints with incomplete information.

Please take into account that the evaluation is run by external experts in the field of security and digital solutions and we do not interfere with their assessment, therefore we will not evaluate complaints related to the results of the evaluation other than related to the mistakes in the evaluation of the eligibility criteria and/or pre-scoring.

## 7. Last but not least - final provisions

Any matters not covered by this Guide will be governed by Polish law and rules related to the Horizon 2020 programme and European Union grants regulations.

We do our best to keep all the applicant data confidential. However, to avoid any doubts, you are entirely responsible to indicate what information is confidential.

Your IPR will remain your property.

For the selected beneficiaries, the agreement will include the set of obligations towards the European Commission (for example: promoting the project and giving visibility to the EU funding, maintaining confidentiality, understanding potential controls by the EC/ECA and OLAF, providing non-confidential information /summary on the project that receives financial support).

The SecurIT Consortium might cancel the call at any time, change its provisions or extend it. In such a case we will inform all applicants about such change. Signature of the agreement is an initial condition to establish any obligations among applicants and any Consortium partners (with respect to the obligation of confidentiality of the application).

You didn't find what you were looking for? You may want to check our [Frequently Asked Questions Section](#).

## 8. Extra hints before you submitting your proposal

A proposal takes time and effort and we know it. Here a few crucial points you should read before hitting the "Submit" button in order to maximise your chances of success:

- Is your project in line with what SecurIT is looking for? Not 100% sure? You can consult this [section](#) as well as this [one](#).
- Did you present your project in a way that will convince evaluators? Go back to this [section](#) if you have any doubt.
- Is your project fulfilling all the eligibility requirements described in the Guide for Applicants? Check again this [section](#).
- Are you able to cope with our signature agreement process and payment arrangements for the selected proposals? You may want to go over this [section](#).
- Did you check our Sub Grant Agreement Template? [Check it here](#).

- Do you need extra help? [Get in touch!](#)

**And as a bonus:** You can read our [R.E.C.I.P.E. for an outstanding European Funding Opportunity application](#) for additional advice. Good luck!

## Annex 1: Information Clause

### Information clause for personal data processing in the 1st Open Call for Applicants organized under SecurIT Project

#### CONTROLLER'S IDENTITY AND CONTACT DETAILS

The data controller is FundingBox Accelerator sp. z o.o. (Al. Jerozolimskie 136, 02-305 Warsaw, Poland).  
In all matters regarding personal data, you can contact us via: [privacy@fundingbox.com](mailto:privacy@fundingbox.com).

#### PURPOSES, LEGAL BASIS AND PROCESSING PERIOD

The purpose and legitimate interest of processing	Legal basis for processing	Period
1) To run an Open Call and collect data necessary to evaluate applications submitted in the Open Call	Legitimate interest of FundingBox (based on Article 6, paragraph 1 (f) of GDPR) which is fulfilling the obligations and our other interests related to these purposes	6 years from the end of the year in which the Project ended
2) To realize the Project goals described in the Grant Agreement (e.g. communication, reporting, collaborating with other project partners)		
3) To consider potential complaints		
4) To gather feedback from applicants when the Open Call is over to improve processes		
If an applicant has been selected to become the beneficiary of the project:		
5) To collect the applicant's details and documentation necessary to verify its legal status. Data will be collected in separate form via FundingBox platform.	Processing is necessary for the performance of a contract (based on Article 6, paragraph 1 (b) of GDPR)	

#### DATA RECEIVERS



Data controller will transfer personal data only to trusted recipients such as entities belonging to the FundingBox's capital group, IT service providers, accountants, law firms, postal and courier companies (who process personal data on the controller's behalf).

Due to the fact that we use the services of Google LLC, your data may be transferred to the USA. We have concluded an agreement with those entities - the so-called Standard Contractual Clauses. This means that in accordance with the decision of the European Commission No. 2021/914 EU of June 4, 2021, your personal data may be processed by this company in the USA. More information about the decision at: <https://fundingbox.com/trust/transfer-outside-eea/>

To realize the Project, data can be transferred also to Project Partners (complete list of the project partners is available at the email address: [privacy@fundingbox.com](mailto:privacy@fundingbox.com)) and European Commission.

## RIGHTS OF DATA SUBJECT

Due to the fact that we process your personal data, you have the right to:

- 1) request access to your personal data,
- 2) demand the rectification of your personal data,
- 3) request to remove or limit the processing of your personal data,
- 4) data portability,
- 5) complain with the supervisory authority (The President of the Personal Data Protection Office, Warsaw, Poland, <https://uodo.gov.pl/en>).

You also have a right to object to processing of your personal data for all purposes indicated above (according to the Article 21 of GDPR).

## INFORMATION ABOUT VOLUNTARY OR OBLIGATORY DATA PROVISION

Providing data is voluntary, although it is necessary to participate in the Open Call. Without providing your data, it is not possible to contact you and evaluate the application.

## Annex 2: SecurIT Challenges and areas of needs

### Table of challenges to be addressed

	Sub-domains	N°	Challenges and potential areas of needs	Examples and illustrations for applicants
Domain #1: sensitive infrastructure protection	Cybersecurity	1	<b>Development of cybersecurity solutions for sensitive infrastructure protection</b>	<p>To propose effective solutions for:</p> <ul style="list-style-type: none"> <li>- Cybersecurity of information and communication systems; Data protection; electromagnetic protection;</li> <li>- Cyber Security incident management;</li> <li>- Cybersecurity - Automatic attack detection and remediation;</li> <li>- Quantum - Post Quantum;</li> <li>- Security Bill of Materials - Device - IoT Security - Shared Responsibility;</li> <li>- Secure Sovereign Cloud.</li> </ul>
	Operations	2	<b>Optimisation of communication networks and alert systems</b>	To optimize solutions for better communication networks (assess, detect and alert both operational forces, LEA or emergency services), the hyper vision and command systems and alert systems.
	Identification and access control	3	<b>Development and optimization of identification and access control for rapid access in the site, all while ensuring that no one and nothing that enters poses a security risk</b>	<p>To propose innovative solutions to identify, provide entry for and inspect individuals, vehicles and goods requesting access to the site such as:</p> <ul style="list-style-type: none"> <li>- Access control for people;</li> <li>- Biometrics &amp; multi biometric systems;</li> <li>- Vehicle control &amp; inspection;</li> <li>- Detecting weapons &amp; explosives: stationary or mobile illicit materials like CBRNE (chemical, biological, radiological, nuclear and explosives) and weapons.</li> </ul>



	<p><b>Zone security and perimeter protection</b></p>	<p><b>4</b></p>	<p><b>Development of solutions to detect and locate any intruders that have managed to penetrate the perimeter protection and barriers to block intrusions</b></p>	<p>To propose innovative solutions such as:</p> <ul style="list-style-type: none"> <li>- Data sensors: detectors; system status indicators; IoT;</li> <li>- Video analysis &amp; sensor fusion: deep learning;</li> <li>- Surveillance – Essential components of the decision-making chain are the detection, recognition and identification of land/air/sea vessels and intruders near or inside the protected area – e.g.: optronic solutions; radar sensors; solutions and data processing/analysis software; video protection (embedded AI);</li> <li>- Surveillance Robots: patrol rounds and missions – detection/identification/neutralization of malicious drone;</li> <li>- Securing physical access routes through digital solutions.</li> </ul>
--	--	-----------------	--	--

	Sub-domains	N°	Challenges and potential areas of needs	Examples and illustrations for applicants
<p><b>Domain #2 - Disaster resilience</b></p>	<p><b>Prior to crisis - prediction: Risk knowledge and evaluation</b></p>	<p><b>5</b></p>	<p><b>Optimisation of prediction of disaster</b></p>	<p>To propose innovative solutions to:</p> <ul style="list-style-type: none"> <li>- Enhance exploitation of monitoring data and satellite/remote sensing information as well as artificial intelligence to improve high-level assessment</li> <li>- Production and processing of data by satellite and aerial imagery (UAV/UAS and light aircraft), as well as by sensor networks. This allows for knowledge about areas concerned and potential risks, integrating data about weather and water courses, providing operational maps for decision-makers and rescue managers.</li> <li>- Modelling and geographical information systems: Modelling territories and the simulation of phenomena allow for the substitution of rarely accessible situations by virtual situations in realistic and operational 3D.</li> </ul>

	<p><b>During the crisis: Communication and warning systems</b></p>	<p><b>6 Optimisation of communication and warning systems in case of disaster</b></p>	<p>These communication systems must be easily transportable and easily deployable within a timeframe compatible with operational demands. The requirement is to have means of communication, which are suitable, diversified, and interoperable such as:</p> <ul style="list-style-type: none"> <li>- Technology that enables the management and monitoring of communication from news media, social media, and internal communication sources in a crisis situation</li> <li>- Information vs decision with the support of AI</li> </ul> <p>To propose innovative solutions to improve forecast / early warning systems, advanced data management, Information update.</p>
	<p><b>After the crisis: Post event analysis and recovery</b></p>	<p><b>7 Development of solutions for a better recovery</b></p>	<p>To propose innovation solutions, post crisis and recovery:</p> <ul style="list-style-type: none"> <li>- Robotics to carry out tasks in hazardous areas for humans</li> <li>- UAV/UAS can view an « area of interest » and give a good understanding of the environment and the situation in the area affected by a disaster</li> <li>- Energy and data network reliability, autonomous and decentralized - to ensure the conservation of the security of data in the context of post-disaster.</li> </ul>

	Sub-domains	N°	Challenges and potential areas of needs	Examples and illustrations for applicants
<p><b>Domain #3 - Public spaces protection – major events</b></p>	<p><b>Detection and alert</b></p>	<p><b>8</b></p>	<p><b>Gather and manage real time information</b></p>	<p>To propose innovative solutions to gather and manage real time information such as facial and vehicle recognition; CCTVS &amp; cameras (eg: embedded AI for flow detection and crowd surveillance, smart cameras, etc.), signal jamming devices for drones, wave scanners systems and anomaly detection systems.</p> <p>To propose warning systems such as innovative tools for public and/or geolocation of public and rescue team.</p>

	<p><b>Analysis</b></p>	<p><b>9</b></p> <p><b>Analyse and extract pertinent and potentially crucial information as quickly as possible</b></p>	<p>To propose innovative tools that can be used in real-time mode (alert, surveillance, or intervention) or in delayed mode (intelligence, investigations, e.g.: audio analytics systems, SOP updates, blind-spot mapping, performance analyses and determining training programmes etc.).</p> <p>To propose innovative analysis tools to support the responsible authorities in monitoring the public information space and quickly identifying disinformation threats</p>
	<p><b>Command and control (resource management) and decision- making support</b></p>	<p><b>10</b></p> <p><b>Communication networks and post - event analysis</b></p>	<p>To produce innovative safe tools that support event planning and resource management during the event. Such tool should support:</p> <ul style="list-style-type: none"> <li>- connectivity of different authentication level users;</li> <li>- definition of environment (defining time, uploading geo information, defining roles, etc.);</li> <li>- possibility to see location of resources and communicate with all linked entities directly via safe tool;</li> <li>- possibility to provide visual guidance;</li> <li>- possibility to upload new relevant data and share with respective entities; possibility to manage few events at a time.</li> </ul> <p>To propose innovative solutions for better communication networks, post event analysis</p>
	<p><b>Data protection and cybersecurity – cybercrime</b></p>	<p><b>11</b></p> <p><b>Detection</b></p>	<p>To propose innovation solutions such as:</p> <ul style="list-style-type: none"> <li>- AI manipulated content analysis: deep fake video detection; deep fake audio detection</li> <li>- Methods for identifying information sources / provenance of information: detection of similar information appearing in different venues / platforms; attribution of information to a single source</li> <li>- Media forensics: image forensics (content manipulation detection; copy-move, splicing, inpainting, enhancement)</li> <li>- Video forensics (content manipulation detection; traditional cut, delete, paste attacks, copy-move, splicing, inpainting, enhancement); audio forensics (content manipulation detection, traditional cut, delete, paste attacks)</li> <li>- Textual content analysis: Image content analysis; Audio content analysis; Video content analysis</li> </ul> <p>Security bills of materials device IoT security shared responsibility</p>