Horizon Europe Cluster 3 Civil Security for Society

Beginners' Guide

Dear reader,

Don't let the following pages discourage you from participating in the Horizon Europe Programme. There is a lot of information, but a beginner certainly doesn't need to consume it all at once. One does not become an expert overnight!

In all participating countries, you could find assistance, the National Contact Point (NCP), who helps you find your way around. The NCP will explain what is necessary for a beginner, recommend practical guides and events to attend and how to prepare for them.

You will need to acquire the basic vocabulary for communication in a proposal preparation environment, such as work programme, call, deadline, type of action, and essential terms from the administrative and budgeting areas. Every NCP has the proper knowledge and is here to help you with all of this.

This beginner's guide will briefly introduce the entire HE programme and focus more on Cluster 3 - Civil Security for Society. In addition, this guide explains selected concepts and the inherent elements and processes of preparing a project proposal and includes basic references.

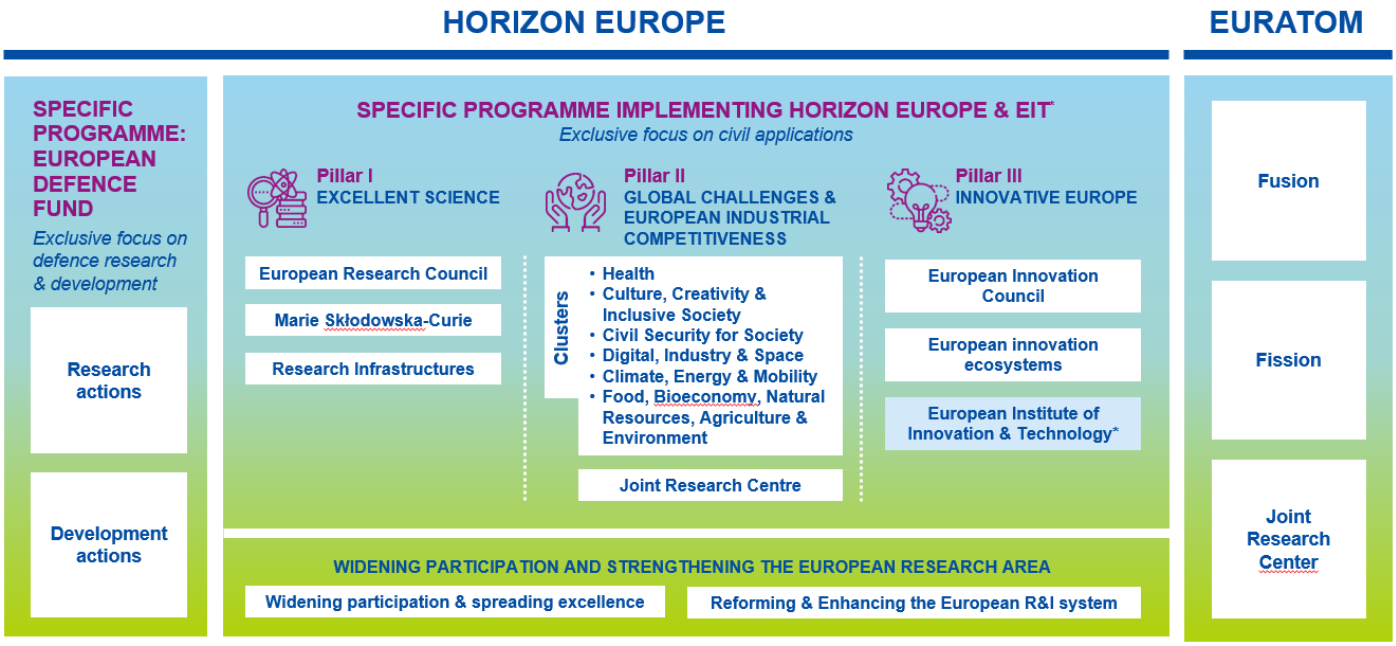
HORIZON EUROPE IN BRIEF

Horizon Europe is the new EU research and innovation Framework Programme (2021-2027) of the European Commission. With a budget of € 95.5 billion, Horizon Europe aims:

- to strengthen the EU's scientific and technological bases and the European Research Area (ERA)
- to boost Europe's innovation capacity, competitiveness, and jobs
- to deliver on citizens' priorities and sustain our socio- economic model and values

@SEREN4_H2020 /company/seren4

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 786680



Similarly to Horizon 2020, the new Framework Programme (FP) is mainly based on 3 pillars:

- Pillar 1: Excellent Science
- Pillar 2: Global Challenges and European Industrial Competitiveness
- Pillar 3: Innovative Europe

New elements in Horizon Europe:

- European Innovation Council: Support for innovations with potential breakthrough and disruptive nature with scale-up potential that may be too risky for private investors. This is 70% of the budget earmarked for SMEs.
- Missions: Sets of measures to achieve bold, inspirational and measurable goals within a set timeframe. There are 5 main mission areas as part of Horizon Europe.
- Open science policy: Mandatory open access to publications and open science principles are applied throughout the programme.
- New approach to partnerships: Objective-driven and more ambitious partnerships with industry in support of EU policy objectives.

This guide will be focusing on Pillar 2 and specifically on the Cluster 3 - Civil Security for Society, the former Societal Challenge 7 (SC7) “Secure Societies – Protecting Freedom and security of Europe and its citizens” in Horizon 2020.

CLUSTER 3 IN BRIEF

Cluster 3 – Civil Security for Society, with a total budget of 1.6 billion euros in seven years has the aim to support wider EU responses to security challenges. It will address capability gaps and different security threats like terrorism and crime, including cybercrime, as well as natural and man-made disasters.

Specifically, Cluster 3 is based on the following specific areas called **Destinations**:

- Destination 1: Better protect the EU and its citizens against Crime and Terrorism
- Destination 2: Effective management of EU external borders
- Destination 3: Resilient Infrastructure
- Destination 4: Increased Cybersecurity
- Destination 5: Disaster-Resilient Society for Europe
- Destination 6: Strengthened Security Research and Innovation

DESTINATION 1: BETTER PROTECT THE EU AND ITS CITIZENS AGAINST CRIME AND TERRORISM

One of the main purposes of this Destination is to contribute significantly to the implementation of the Security Union Strategy , i.e. to include Research and Innovation as one of the key building blocks enabling the achievement of the overall policy objectives. As such, the topics in this Destination aim at fully addressing all the key issues underlined in the Strategy. In addition, this Destination touches upon the Counter-Terrorism Agenda as well as the security dimension of the New Pact on Migration and Asylum, notably the issues related to criminal networks.

The goal of this Destination is to bring improved prevention, investigation and mitigation of impacts of crime, including of new/emerging criminal modi operandi (such as those exploiting digitisation and other technologies). Research and innovation will support Police Authorities and, when applicable, other relevant end-users in better tackling crime, including cybercrime, and terrorism as well as different forms of serious and organised crime. Projects within this Destination will also deliver operational tools for enhanced criminal investigation capabilities for Police Authorities and, when applicable, other relevant end-users. Furthermore, this Destination aims at improved security of public spaces and public safety, while at the same time preserving the open nature of urban public spaces.

Proposals for topics under this Destination should set out a credible pathway to contributing to the following expected impact of the Horizon Europe Strategic Plan 2021-2024: “Crime and terrorism are more effectively tackled, while respecting fundamental rights, […] thanks to more powerful prevention, preparedness and response, a better understanding of related human, societal and technological aspects, and the development of cutting-edge capabilities for police authorities […] including measures against cybercrime."

DESTINATION 2: EFFECTIVE MANAGEMENT OF EU EXTERNAL BORDERS

This Destination addresses, among other, objectives identified by the Security Union Strategy as well as the border management and security dimensions of the New Pact on Migration and Asylum.

Topics included under the Destination are aimed at ensuring strong European land, air and sea external borders. This includes by developing strong capabilities for checks at external borders hence safeguarding the integrity and functioning of the Schengen area without controls at the internal borders, by compensating the absence of intra-EU border checks; being capable to carry out systematic border checks, including identity, health and security checks as necessary, while facilitating the travel of bona fide travellers and respecting rights and possible vulnerabilities of individuals; providing integrated and continuous border surveillance, situational awareness and analysis support; combating identity and document frauds; supporting future technology for the European Border and Coast Guard; supporting the interoperability and performance of EU data exchange and analysis IT systems; supporting better risk detection, incident response and crime prevention; improving European preparedness to, and management of, future rapidly evolving changes; and updating our maritime security management including migration, trafficking as well as search and rescue capabilities.

Proposals for topics under this Destination should set out a credible pathway to contributing to the following expected impact of the Horizon Europe Strategic Plan 2021-2024: “Legitimate passengers and shipments travel more easily into the EU, while illicit trades, trafficking, piracy, terrorist and other criminal acts are prevented, due to improved air, land and sea border management and maritime security including better knowledge on social factors."

DESTINATION 3: RESILIENT INFRASTRUCTURE

The Security Union Strategy identifies the protection of critical infrastructures as one of the main priorities for the EU and its Member States for the coming years. Specific reference is established to growing interconnectivity as well as emerging and complex threats: technological trends like the use of Artificial Intelligence and the rapid development of sophisticated unmanned vehicles, the impact of natural and man-made disasters, as well as major crisis scenarios like the COVID-19 pandemic and unexpected events.

Infrastructure resilience and protection is a domain affected by various global developments and thus needs to be supported by targeted security research. Technological complex applications that offer the possibility for better prevention and preparedness can enable efficient response to different threats and fast recovery. Physical, Cyber and Hybrid attacks are of particular relevance in the overall risk scenarios, since they are designed to target vulnerabilities and aim in many cases at disrupting infrastructure and its services.

Proposals for topics under this Destination should set out a credible pathway to contributing to the following expected impact of the Horizon Europe Strategic Plan 2021-2024:“[…] resilience and autonomy of physical and digital infrastructures are enhanced and vital societal functions are ensured, thanks to more powerful prevention, preparedness and response, a better understanding of related human, societal and technological aspects, and the development of cutting-edge capabilities for […] infrastructure operators […]"

DESTINATION 4: INCREASED CYBERSECURITY

Cybersecurity research and innovation activities will support a Europe fit for the digital age, enabling and supporting digital innovation while highly preserving privacy, security, safety and ethical standards. They will contribute to the implementation of the digital and privacy policy of the Union in particular the NIS Directive, the EU Cybersecurity Act, the EU Cybersecurity Strategy, the GDPR, and the future e-Privacy Regulation.

Proposals for topics under this Destination should set out a credible pathway contributing to the following impact of the Strategic Plan 2021-2024: "Increased cybersecurity and a more secure online environment by developing and using effectively EU and Member States' capabilities in digital technologies supporting protection of data and networks aspiring to technological sovereignty in this field, while respecting privacy and other fundamental rights; this should contribute to secure services, processes and products, as well as to robust digital infrastructures capable to resist and counter cyber-attacks and hybrid threats".

DESTINATION 5: DISASTER-RESILIENT SOCIETY FOR EUROPE

This Destination supports the implementation of international policy frameworks (e.g. the Sendai Framework for Disaster Risk Reduction, the Paris Agreement, Sustainable Development Goals), EU disaster risk management policies tackling natural and man-made threats (either accidental or intentional), European Green Deal priorities including the new EU Climate Adaptation Strategy,, as well as the Security Union Strategy and the Counter-Terrorism Agenda.

The implementation of international policy frameworks requires cross-border and cross-sectoral cooperation an enhanced collaboration among different actors and strengthened knowledge covering the whole disaster management cycle, from prevention and preparedness to response and recovery (and learning). Understanding and exploiting the existing linkages and synergies among policy frameworks represents in this sense a global priority for future research and innovation actions in the field of natural hazards and man-made disasters.

Proposals for topics under this Destination should set out a credible pathway to contributing to the following expected impact of the Horizon Europe Strategic Plan 2021-2024: "Losses from natural, accidental and man-made disasters are reduced through enhanced disaster risk reduction based on preventive actions, better societal preparedness and resilience and improved disaster risk management in a systemic way."

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 786680

DESTINATION 6: STRENGTHENED SECURITY RESEARCH AND INNOVATION

This Destination has been designed with the purpose to serve equally to all the expected impacts of Cluster 3. Research applied in this domain will contribute to increasing the impact of the work carried out in the EU Security Research and Innovation ecosystem as a whole and to contribute to its core values: Ensuring that security R&I maintains the focus on the potential final use of its outcomes; Contributing to a forward-looking planning of EU security capabilities; Ensuring the development of security technologies that are socially acceptable; Paving the way to the industrialisation, commercialisation, acquisition and deployment of successful R&I outcomes; Safeguarding the open strategic autonomy and technological sovereignty of the EU in critical security areas by contributing to a more competitive and resilient EU security technology and industrial base.

While the other Destinations offer research and innovation activities to develop solutions to address specific security threats or capability needs, this Destination will contribute with instruments that will help bringing these and other developments closer to the market. Such instruments will help developers (including industry, research organisations and academia) to improve the valorisation of their research investment. They will also support buyers and users in materialising the uptake of innovation and further develop their security capabilities.

RELATED PROGRAMMES

Several programmes within Horizon Europe and across Europe are either linked or related to the Civil Security Programme. It can be helpful for you to be aware of that, both regarding opportunities and an overview of Europe's focus.

- Horizon Europe – synergies with other clusters and programmes
  - Culture, Creativity & Inclusive Society
  - Digital, Industry and Space
  - Climate, Energy and Mobility
- Horizon Europe Partnerships
- Missions
- Other European programmes
  - Internal Security Fund
  - Digital Europe
  - European Defence Fund
  - Programmes by DG ECHO

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 786680

WRITING A PROPOSAL IN HORIZON EUROPE

We advise you to carefully read the call and topic description in the work programme. Understanding the topic of the call in detail is essential to prepare a competitive project proposal. Make sure your project idea will address the scope of the topic and contribute to the expected outcome described in the work programme. Other aspects you have to be aware of are the eligibility conditions. Cluster 3 is specific as it imposes additional requirements like active participation of a minimum number of practitioners in the proposal in many topics. It is also necessary to understand the difference between different types of projects that occur in the programme as this potentially, among other things, bring different funding rates. You should also understand the rules for participation, policies behind the topics, what has already been achieved in the respective research field, horizontal issues, and other aspects of the Horizon Europe programme, which we elaborate more on the following pages.

All relevant information for a preparation of a succesful proposal is available on Funding and Tender Opportunities Portal.

What are the most common types of projects occurring in the Work Programme?

The most common types of projects in the Cluster 3, in the Horizon Europe terminology called actions, are Research and Innovation Actions, Innovation Actions, Coordination and Support Actions and Pre-commercial procurement actions:

- **Research and Innovation Action (RIA):** include activities that aim primarily to establish new knowledge or to explore the feasibility of a new or improved technology, product, process, service or solution. This may include basic and applied research, technology development and integration, testing, demonstration and validation of a small-scale prototype in a laboratory or simulated environment. Funding rate: 100%
- **Innovation Action (IA):** include activities that aim directly to produce plans and arrangements or designs for new, altered or improved products, processes or services. These activities may include prototyping, testing, demonstrating, piloting, large-scale product validation and market replication. Funding rate: 70% (except for non-profit legal entities, where a rate of up to 100% applies).
- **Coordination and Support Action (CSA):** include activities that contribute to the objectives of Horizon Europe. This excludes R&I activities. Also eligible are bottom-up coordination actions which promote cooperation between legal entities from Member States and Associated Countries to strengthen the European Research Area, and which receive no EU co-funding for research activities. Funding rate: 100%

- **Pre-commercial procurement action (PCP):** include activities that aim to help a transnational buyers' group to strengthen the public procurement of research, development, validation and, possibly, the first deployment of new solutions that can significantly improve quality and efficiency in areas of public interest, while opening market opportunities for industry and researchers active in Europe. Eligible activities include the preparation, management and follow-up, under the coordination of a lead procurer, of one joint PCP and additional activities to embed the PCP into a wider set of demand-side activities. Funding rate: 100% (other funding rates may be set out in the specific call conditions).

What does the TRL mean?

NASA first introduced a Technology Readiness Level (TRL) in the 1970s, and in European research and innovation framework programmes, it was first time used in 2014 under Horizon 2020 programme. TRL represents a method for assessing and indicating the maturity level of technology to which the project relates. Technology oriented Horizon Europe calls provide information to which TRL the technology has to be moved during the implementation of the project. Horizon Europe programme defines nine technological readiness levels, with actions to support each, from funding basic research to commercializing innovation. Where the specific call conditions require the TRL, the following definitions apply, unless otherwise specified:

- **TRL 1** — Basic principles observed
- **TRL 2** — Technology concept formulated
- **TRL 3** — Experimental proof of concept
- **TRL 4** — Technology validated in a lab
- **TRL 5** — Technology validated in a relevant environment (industrially relevant environment in the case of key enabling technologies)
- **TRL 6** — Technology demonstrated in a relevant environment (industrially relevant environment in the case of key enabling technologies)
- **TRL 7** — System prototype demonstration in an operational environment
- **TRL 8** — System complete and qualified
- **TRL 9** — Actual system proven in an operational environment (competitive manufacturing in the case of key enabling technologies, or in space)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 786680

Bakground Information

Preparing a proposal for Horizon Europe is a long and arduous process. Therefore, it is crucial to be prepared and do thorough background work to become successful.

As mentioned before, it is essential to understand the specific Work Programme. It is crucial to familiarize yourself with the Horizon Europe Strategic Plan and use it as a reference when preparing a proposal. The Strategic Plan gives directions to the content of the Work Programme for the period 2021-2024 and sets out four key strategic orientations for R&I that are supported by 15 impact areas. The Civil Security programme addresses two key strategic orientations:

- **Promoting an open strategic autonomy by leading the development of key digital and enabling technologies, sectors and value chains** to accelerate and steer the digital and green transitions through human-centred technologies and innovations. The impact areas that fall under this key area are:
  - A competitive and secure data-economy;
  - Industrial leadership in key and emerging technologies that work for people;
  - Secure and cybersecure digital technology;
  - High quality digital services for all.
- **Creating a more resilient, inclusive and democratic European society, prepared and responsive to threats and disasters, addressing inequalities** and providing high-quality health care, and empowering all citizens to act in the green and digital transitions. Impact areas that fall under this key area are:
  - A resilient EU prepared for emerging threats
  - A secure, open and democratic EU society
  - Good health and high-quality accessible healthcare
  - Inclusive growth and new job opportunities

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 786680

Identify the apropriate call

Since the structure of the Topics follows a top-down approach, in the sense that the European Commission explicity include the requirements and the related expectations, it is highly recommended that applicants carefully read the entire specific Work Programme Civil Security for Society 2021-2022, in which they can find all the information about the policy context, the scope of the calls, the budget allocated to each topic, some additional condition for the participation and eligibility, indicative publications and the deadlines of calls.

Standard Proposal Template

The standard length of a proposal in Horizon Europe is 45 pages for the RIA and IA projects and 30 pages for the CSA projects. The proposal consists of two parts:

- Part A contains of the administrative information entered by the participants through the submission system in the Funding & Tenders Portal. It includes a description of the partners, a table of researchers, and each participating organisation's role. In part A, partners specify whether they have a gender equality plan and give information about ethics and security. The participants can update the information in the submission system at any time before final submission.
- Part B of the proposal is the narrative part, the project's technical description, which includes three sections corresponding to the evaluation criteria. Part B is uploaded as a PDF document using the templates (RIA and IA, CSA, PCP) downloaded from the submission system in the Funding & Tenders Portal for the specific call or topic.

Templates for specific calls may slightly differ from what has been described here.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 786680

Putting together a Consortium

Any entity can be part of a consortium, but a consortium needs to include three independent legal entities *each established in a different Member State or associated country and with at least one of them established in a Member State.*

Putting together a strong consortium is an important part for a successful proposal. Applicants need to think about the roles each partner can play in the project and how they complement each other, are there any knowledge gaps, are leading entities in the field missing from the proposal, do the involved entities cover the whole value chain?

Essential partners in security research projects that can be involved in consortia:

- resarchers
- large industry and SMEs
- practitioners (their involvement is often mandatory in the Security topics)
- policy makers
- citizens/end users (their involvement is important for the implementation of the project and delivery of the project results and expected outcomes)

Horizontal issues

It is important for applicants to familiarize themselves with horizontal issues that include Open Science, Ethics and Security, Gender issue, Intellectual Property Rights (IPR) and Standardization.

- **Open Science** is a system change allowing for better science through open and collaborative ways of producing and sharing knowledge and data, as early as possible in the research process, and for communicating and sharing results.

  The Commission has launched a publishing platform Open Research Europe for scientific papers resulting from Horizon 2020 and Horizon Europe funding that will be open and accessible. The platform will contribute to open, fast and cost-efficient scientific publications and make it easier to beneficiaries of Horizon 2020 and Horizon Europe to comply with the relevant open access terms of their funding.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 786680

- For all activities funded by the European Union, **Ethics and Security** is an integral part of research from beginning to end, and ethical compliance is seen as pivotal to achieve real research excellence.
- **Gender Equality** policies and the gender dimension in research and innovation are crucial for the future Framework Programme and should be adequately reflected and integrated into the official documents as well as in further discussion, dissemination, and visibility.

  In Horizon Europe, the gender dimension becomes increasingly important and this is evident since the European Commission developed a New Gender Equality Strategy 2020-2025**.** The strategy requires that the Horizon Europe applicants have to provide in the proposal preparation a **gender equality plan** (starting from 2022 calls).
- **Intellectual Property** issue is a key driver for the exploitation of projects' results and consequently for the economic growth of the European Union. For this reason, the European Commission has published an action plan covering IP issues issues in order to support enterprises (especially SMEs) in efficiently exploiting their inventions, contemporary improving the European economy and society. For applicants it is crucial to include the Intellectual Property issue in any phase of the project (from the proposal phase to the end of the project and beyond) in order to protect their innovative creations.
- **Standardisation** plays a vital role in eliminating technical trade barriers and facilitate market access. Standards also help ensure that complementary products and services are interoperable, facilitate the introduction of innovative products and ultimately build trust in the quality of products and services. This is the reason why to include standardisation the research project. You can learn more about how standardisation can support researchers and innovators or read the SEREN4 Infosheet on standardisation.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 786680

Financial rules

Changes have been made regarding financial rules from Horizon 2020 to Horizon Europe. The rules have been simplified to increase legal certainty and the aim is to reduce administrative burden of beneficiaries.

- Single set of rules for all EU funding Programmes.
- Cost categories: personnel costs, subcontracting costs, purchase costs, other cost, indirect cost
- Personnel cost – calculation will be based on daily rates instead of hourly rate.
- Affiliated entities in Horizon Europe used to be Linked third parties in Horizon 2020. These are “entities that have link with the beneficiary, in particular legal or capital link, which is neither limited to the action nor established for the sole purpose of its implementation".
- Introduction of Associated Partner which was international partner in Horizon 2020. Associated partner performs work but cannot declare costs, it can be linked to one or more beneficiaries or with the whole consortium.

For more information

Annotated model grant agreement

Rules for participation

Open Science

Open Research Europe

Ethics

Gender equality strategy

IP in Horizon Europe

Standardisation

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 786680

SUBMISSION OF THE PROPOSAL IN HORIZON EUROPE

Once the proposal is ready, the Coordinator must submit it to the European Commission within the deadline of the Call. In continuity with Horizon 2020, in Horizon Europe the submission procedure is entirely online, through the Funding and Tender Opportunities Portal: the single-entry point for the Framework Programmes of the European Commission.

Applications must be readable, accessible and printable.

Before submitting the proposal, applicants should verify that all the administrative requirements have been satisfied (otherwise the proposal will not be evaluated).

For instance, this may regard the page limit. Please remember that **in Horizon Europe the limit is 45 pages for the full application** (except for the Coordination and Support Actions, where the page limit is 30 pages).

EVALUATION OF THE PROPOSALS IN HORIZON EUROPE

The evaluation process in Horizon Europe will be based on fair, transparent and objective procedures. The entire process (from application to signing the grant agreement) is managed electronically through the Funding and Tender Portal. The evaluation itself will be performed by independent experts. The experts represent the EC who is funding your project. Their task is to make an expert assessment of the proposal according to predefined criteria. In their evaluation, among other things, they focus on the project's scientific quality, the methodology for achieving the results and pathways to achieve the expected outcomes and impacts.

As for the evaluation criteria, they are three: **Excellence, Impact and Quality of Implementation**. The evaluation criteria for the different funding types are described in detail in the evaluation forms: RIA and IA, CSA, PCP and PPI. In particular, the European Commission revised the impact criteria following a clear logic linking the project results to the expected outcomes over the medium term, and to the wider long-term impacts, as specified in the work programme. Applicants have to describe a plausible pathway to scientific, societal and economic impact over time, including beyond the lifetime of a project.

The threshold for individual criteria will be 3. The overall threshold, applying to the sum of the three individual scores, will be 10. To determine the ranking for 'Innovation actions', the score for 'Impact' will be given a weight of 1.5.

Proposals that pass both the individual threshold AND the overall threshold will be considered for funding within the limits of the available call budget. Other proposals will be rejected.

Experts also assess each project selected for funding during the evaluation phase from the ethics (ethical appraisal procedure) and security (security scrutiny) perspective. The seriousness of the issue governs the depth of the assessments. You may find more information about the security assessment in the Annex of this guide and about the ethics assessment in the document "How to complete your ethics self-assessment".

TIPS FROM NCPs

National Contact Points have valuable experience and insight into what successful proposals should include and how to prepare for a proposal writing. Below are several recommendations from NCPs around Europe.

- Get familiar with the EU Portal and register your organisation at an early stage (the validation needs some time).
- Make use of all supporting information and documents. Your local National contact point (NCP) will support you!
- Check for Match Making, Networking and Brokerage events that will help you find project partners.
- Start early to integrate end-users into your consortium.
- Involve actors from different organisations along the value chain!
- Get informed about specific policy backgrounds and practitioner needs.
- Make sure you address the scope of the topic and the expected outcome.
- Ensure that your idea is “beyond state of the art” and unique.
- Build on previous successful EU projects (CORDIS, Horizon Dashboard).
- Identify solutions available to address the security gaps.
- Demonstrate well the possible impact of your project and how to bring solutions to the market.
- Consider the impact of your project on civil society and how to address civil society needs.
- Protect your research results from misuse and unauthorised disclosure (Security Appraisal).
- Address standardisation needs.
- Check all mandatory criteria, balance budgets and countries and entities.
- Do not use too much jargon. All acronyms must be introduced - use them to abbreviate only.
- Avoid duplication.
- Illustrate your project idea by using appropriate diagrams.
- The text should be well written - the evaluator reads each text in few hours and possibly several proposals per day. Respect the page limit!
- Frequently evaluators represent end-users, societal groups and other experts in your research field. Make sure that they will see the added value of your research!
- Remember what is asked for in the call text. Know who the end-users are and how they can benefit from your solution.
- Ask someone who is not involved in your project to read the proposal before submitting it.

ANNEX Cluster 3 specifics

Beneficiaries, when written in the Topic text, have to include end-users in the consortium, or so-called **practitioners** (police authorities, border guards, first responders, operators of critical infrastructure, firefighters, civil protection, etc.). This must be documented in a specific table added as an Annex to the proposal part B to not count against the page limits. The involvement of practitioners has through the years proven its value, ensuring that the results of the projects meet the needs of the end-users. The inclusion in the project consortium therefore continues to be of fundamental importance and represents an additional **eligibility criteria**, non-compliance makes the proposal ineligible for funding. The details are described in the *"conditions of the call"* section of the Work Program.

Programme Security Instruction for Horizon Europe

Programme Security Instruction (PSI) establishes the security procedures to be applied and the common security procedures and processes to be followed for the management of a classified grant awarded under the Horizon Europe Programme, as well as assigns the responsibilities for the protection of classified information generated or exchanged in connection with the Programme.

How to handle security-sensitive projects

Short guide covering the proposal stage, grant preparation stage and the project implementation of Horizon Europe. EU classification is normally needed if activity concerns a security-sensitive subject matter and falls under one of the security-sensitive types of activities. The precise **details and cases vary by EU Programme.** For more information and examples, see the Guidelines on the classification of information in Horizon Europe projects; Classification of information in Digital Europe projects and Classification of information in EDF projects.

Classification of information in Horizon Europe projects

Initial version of the Guide was published in 2013. Updated guide explains when and for how long information has to be classified, the different classification levels and how to classify information in different types of research (CBRN, explosive, critical infrastructures, terrorism, boarder security, organised crime, digital security and space)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 786680

Proposal template: Part B - Security Section

The Security Section must be completed in accordance with the guidance How to handle security-sensitive projects and Classification of information in Horizon Europe projects. The form also includes instructions for preparing a Security Aspects Letter (SAL).

> **Security Aspect Letter** (SAL): if your project intends to use or produce classified information, you have to fill in the SAL (a part of proposal template in security section), according to your project-specific security requirements. Consult the guidance Classification of information in Horizon Europe projects. The security aspects letter (SAL) is an integral part of the classified grant agreement and describes grant agreement specific security requirements.
>
> **Security Classification Guide** (SCG)*:* is a document (Annex of the SAL) which describes the elements of a project or grant agreement which are classified, specifying the applicable security classification levels. The SCG lists classified deliverables as defined in a security scrutiny procedure. The SCG issued to Beneficiaries may be modified throughout the life of the grant agreement and the classified elements may be re-classified or downgraded. The SCG also includes, if applicable, an informative list of Classified Background Information used.

Security scrutiny: is a procedure to ensure sufficient protection of classified information in EU grants. It is implemented for projects selected for funding. If the scrutiny leads to requirements to be implemented before grant signature, you will need to take immediate action to comply. If the scrutiny leads to classification and additional requirements to be fulfilled during the project, this will be automatically reflected in the system (classification of existing deliverables, Security Aspect Letter (SAL), Security Classification Guide (SCG), additional security deliverables and security requirements work package).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 786680