eNewsletter August 2021

# Horizon Europe Cluster 3

## Content



contact@seren-project.eu

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

# 1. Useful documents for the proposal preparation

Below you can find some information that we consider useful for the preparation of your proposal.

### 1.1. Programme Security Instruction for Horizon Europe

Programme Security Instruction for Horizon Europe (PSI) represents 81 pages of helpful information. This PSI establishes the security procedures to be applied and the standard security procedures and processes to be followed to manage 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.

### 1.2. Classification of information in Horizon Europe projects

Classification of information in Horizon Europe projects was initially published in 2013. This updated guide explains when and for how long the information has to be classified, the different classification levels and how to classify information in different cases of research (explosive, CBRN, critical infrastructures, terrorism, boarder security, organised crime, digital security and space).

### 1.3. How to handle security-sensitive projects

How to handle security-sensitive projects guide covers proposal stage, grant preparation stage and the Horizon Europe project implementation. 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 European Defence Fund projects.

### 1.4. Proposal template: Part B Security Section

The Security Section of the proposal template Part B 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),



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

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 classified elements of a project or a grant agreement (deliverables) 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.

### 1.5. Security Scrutiny

Security Scrutiny ensures 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).

### 1.6. Guidance notes for misuse of research results

Guidance notes for misuse of research results will be available soon.

### 1.7. Annotated Model Grant Agreement

Annotated Model Grant Agreement (AGA) is a user guide that aims to explain to applicants and beneficiaries the EU Model Grant Agreements (General MGA, Lump Sum MGA, Unit MGA, Operating Grants MGA and Framework Partnership Agreement) for the EU funding programmes 2021-2027.

Programme specificities are reflected in this document as examples — in so far as they are accepted as mainstream solutions that can be used by several EU programmes. The purpose of this document is to help users understand and interpret their Grant Agreements (GAs). By avoiding technical vocabulary, legal references and jargon, it seeks to help readers find answers to the practical questions they may come across when setting-up or implementing their projects. In the same spirit, the document's structure mirrors that of the EU Model Grant Agreements (MGAs). It explains each MGA Article and includes examples where appropriate.



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

### 1.8. Ethics guide: How to complete your ethics self-assessment

A new version of the Ethics guide: How to complete your ethics self-assessment is available on the Funding and Tender Opportunities Portal. Data for Digital Europe programme and European Defence Fund were integrated. The Ethics Guide now also includes a section on Artificial Intelligence solutions in projects. It explains the basic principles of its ethical use. It also refers to the Ethics Guidelines for Trustworthy AI (available in all languages) prepared by independent experts. In this context, we draw your attention to the draft of the new "AI Regulation", described separately in this Newsletter.

Information about Key changes to the ethics appraisal process in HE can be obtained at an interesting EC workshop (130miutes), where 40 minutes are devoted to the issue of ethics in the use of artificial intelligence.

## 2. EC proposal of the Artificial Intelligence systems "AI Regulation"

On 21 April 2021, the European Commission (EC) published its proposal for a Regulation on Artificial Intelligence (the "AI Regulation"). This proposal results from several years of work of the European Commission, including a "White Paper on Artificial Intelligence" and broad public consultation. We wrote about the initial documents on AI in the SEREN4 Newsletter, April 2020. Furthermore, the EC proposal is based on the EU Parliament's October 2020 legislative proposal to create a legal and ethical framework/rules for the rapid development and deployment of AI.
The proposal contains recommendations for several regulatory measures and definitions of the terminology used. It aims to establish a legal framework necessary to facilitate innovation and investment in AI. Furthermore, the new Regulation should ensure safe and trustworthy use of AI applications while maintaining a code of ethics.

The main provisions of the AI Regulation are the introduction of:

- **Binding rules** for AI systems that apply to providers, users, importers, and distributors of AI systems in the EU, irrespective of where they are based;
- A list of specific **prohibited** AI systems;
- Extensive **compliance obligations** for high-risk AI systems;

Article 3 of the General Provision brings definitions of the **terminology** used, for example:

- **Artificial intelligence system** (AI system) means software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with;



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

- **Intended purpose** means the use for which an AI system is intended by the provider, including the specific context and conditions of use, as specified in the information supplied by the provider in the instructions for use, promotional or sales materials and statements, as well as in the technical documentation;
- **Reasonably foreseeable misuse** means the use of an AI system in a way that is not in accordance with its intended purpose, but which may result from reasonably foreseeable human behaviour or interaction with other systems;
- **Training data** means data used for training an AI system through fitting its learnable parameters, including the weights of a neural network;
- **Validation data** means data used for providing an evaluation of the trained AI system and for tuning its non-learnable parameters and its learning process, among other things, in order to prevent overfitting; whereas the validation dataset can be a separate dataset or part of the training dataset, either as a fixed or variable split;
- **Testing data** means data used for providing an independent evaluation of the trained and validated AI system in order to confirm the expected performance of that system before its placing on the market or putting into service; of undermining fundamental rights and are therefore explicitly prohibited;
- **Biometric data** means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

Examples of other listed term: biometric categorisation system; remote biometric identification system; real-time remote biometric identification system; publicly accessible space; serious incident and many other.

Title II, Article 5 - **Prohibited AI practices** - The proposed AI Regulation lists several AI systems which EC believe bear an unacceptable risk of violating fundamental rights and are therefore explicitly prohibited (ethical consideration). The Regulation contains a proposal for exemptions for LEAs (specific cases of real-time remote biometric identification systems in publicly accessible spaces).

Title III of the Regulation regards **High-risks AI** systems and proposes an approach for their classification and the criteria for the quality and working with data used or generated in these high-risk AI systems and training. The Regulation also contains conditions for technical documentation, record-keeping, transparency and provision of information to users. The proposal also sets out the purpose and requirements for human oversight and covers high-risk AI systems' accuracy, robustness, and cybersecurity. Eight areas of high-risk AI systems use are listed in Annex III of the AI Regulation.

Of course, the proposed AI Regulation has a much broader scope with implications for innovation and future markets. In this article, we have selected only parts where we want to draw the attention of research projects proposers. We consider them essential because the AI systems resulting from the currently prepared projects will be put into practice when the AI regulation is binding.



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

## 3. Participation of Switzerland in Horizon Europe Programme

Entities based in Switzerland can participate in Horizon Europe. However, as Switzerland is considered a non-associated country, Swiss entities (including companies and SMEs) can apply only for Horizon Europe's calls and related programmes and initiatives open to non-associated third country participation.

Legal entities taking part in collaborative projects open to third country participation will receive funding via the State Secretariat for Education, Research and Innovation (SERI) in the same way as it was organised in the past. In addition, a corresponding financial guarantee, which can be shared with the consortium partners, is provided by SERI on its website.

In the new generation of EU Programmes for Research and Innovation, entities from non-associated third countries participate in the collaborative projects as associated partners. The budget of the associated partner is indicated in the project proposal but not taken into account in the project budget and corresponding EC funding.

Participants from non-associated third countries cannot coordinate projects. They can, however, lead work packages as any other participant.

We highly recommend consulting the participation of Switzerland in the 2021 calls for the collaborative proposals with the documents provided by SERI as these documents are constantly updated:

- Information on the Swiss participation in H2020 and HE
- Questions and Answers on the Swiss participation in H2020 and HE

## 4. Galileo/EGNOS and/or Copernicus

In more than 100 topics across Horizon Europe Clusters for 2021-2022 calls, the use of EGNOS and/or Copernicus services and data is considered necessary. Therefore, if projects use the navigation, positioning and other services, including remote sensing, the European Commission mandates the involvement of the European Galileo / EGNOS and Copernicus systems. Galileo/EGNOS and Copernicus data and services are free of charge.

There are 25 such topics in Cluster 3 Work Programme 2021-2022 with the following eligibility condition:
"If projects use satellite-based, positioning, navigation and/or related timing data and services, beneficiaries must make use of Galileo/EGNOS (other data and services may additionally be used). The use of Copernicus for earth observation is encouraged."



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

Cluster 3 Work Programme 2021 with Galileo/EGNOS eligibility condition:

| TOPIC |
|---|
| HORIZON-CL3-2021-FCT-01-07: Improved preparedness on attacks to public spaces |
| HORIZON-CL3-2021-FCT-01-08: Fight against trafficking in cultural goods |
| HORIZON-CL3-2021-FCT-01-09: Fight against organised environmental crime |
| HORIZON-CL3-2021-FCT-01-10: Fight against firearms trafficking |
| HORIZON-CL3-2021-BM-01-01: Enhanced security and management of borders, maritime environment, activities and transport, by increased surveillance capability, including high altitude, long endurance aerial support |
| HORIZON-CL3-2021-BM-01-02: Increased safety, security, performance of the European Border and Coast Guard and of European customs authorities |
| HORIZON-CL3-2021-BM-01-03: Improved border checks for travel facilitation across external borders and improved experiences for both passengers and border authorities' staff |
| HORIZON-CL3-2021-DRS-01-01: Improved understanding of risk exposure and its public awareness in areas exposed to multi-hazards |
| HORIZON-CL3-2021-DRS-01-02: Integrated Disaster Risk Reduction for extreme climate events: from early warning systems to long term adaptation and resilience building |
| HORIZON-CL3-2021-DRS-01-03: Enhanced assessment of disaster risks, adaptive capabilities and scenario building based on available historical data and projections |
| HORIZON-CL3-2021-DRS-01-06: Fast deployed mobile laboratories to enhance situational awareness for pandemics and emerging infectious diseases |

# 5. Social Sciences and Humanities - SSH

Assessing the effective contribution of social science and humanities disciplines and expertise is, in some cases, part of the scientific methodology of the project.

When the integration of SSH is required, applicants have to show the roles of these disciplines or justify if they consider that SSH is not relevant for their project. A proposal without a sufficient contribution/integration of SSH research and competencies will receive a lower evaluation score.

Cluster 3 – WP 2021 - topics flagged as SSH relevant:

| TOPIC |
|---|
| HORIZON-CL3- 2021- CS- 01- 01 Dynamic business continuity and recovery methodologies based on models and prediction for multi-level Cybersecurity |
| HORIZON-CL3-2021-FCT-01-06 Domestic and sexual violence are prevented and combated |
| HORIZON - CL3 2021 FCT 01-07 Improved preparedness on attacks to public spaces |
| HORIZON - CL3 2021 FCT 01 08 Fight against trafficking in cultural goods |
| HORIZON-CL3- 2021- FCT -01-11 Prevention of child sexual exploitation |



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

| |
|---|
| HORIZON-CL3 -2021-FCT-01 -12 Online identity theft is countered |
| HORIZON-CL3 -2021- DRS- 01- 01 Improved understanding of risk exposure and its public awareness in areas exposed to multi-hazards |
| HORIZON-CL3 -2021-DRS -01 -02 Integrated Disaster Risk Reduction for extreme climate events: from early warning systems to long term adaptation and resilience building |
| HORIZON-CL3- 2021-DRS- 01- 03 Enhanced assessment of disaster risks, adaptive capabilities and scenario building based on available historical data and projections |
| HORIZON-CL3-2021- SSRI -01 -02 Knowledge Networks for Security Research & Innovation |
| HORIZON-CL3- 2021- SSRI -01- 05 Security research technologies driven by active civil society engagement: transdisciplinary methods for societal impact assessment and impact creation |

# 6. Cascade Funding

Cascade Funding in Horizon Europe, also known as Financial Support for Third Parties (FSTP), is a European Commission mechanism to distribute funding from the project consortia to the third parties, mainly SMEs, to uptake or develop innovative digital technologies.

Cluster 3 cybersecurity calls 2022 (CS-2022-01-01 and CS-2022-01-03 ) involve possible implementation of FSTP mechanism, in which consortia may publish their own calls for proposals (open calls) and provide financial support in the form of grants. Cascade funding also occurs in other Clusters, but most typically in calls of Cluster 4 (Digital, Industry and Space).



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