Secure Societies SC7 Calls 2019

Security Aspects

Outline

- Context and background
- Legal framework
- Security Scrutiny Procedure
- Implementation of the Security Scrutiny Results
- Issues to address during proposal preparation
- References

Context and background

- Security and the need to protect certain information
- Security measures: e.g. limited dissemination, classification

General Annexes - Annex J. Actions involving classified information

In the case of actions involving security-related activities, special provisions for classified information (as defined in the Commission Rules of Procedure (Decision 2015/444/EC, ECSC, Euratom, and further explained in the Guidelines for the classification of research results) **will be taken in the grant agreement, as necessary and appropriate.**

Proposals should not contain any classified information. **However, it is possible that the output of an action (’results’) needs to be classified, or that classified input ('background') is required**. In such cases proposers have to ensure and provide evidence of the adequate clearance of all relevant facilities. Consortia have to clarify issues such as e.g. access to classified information (…) prior to submitting the proposal. Proposals need to provide a draft security classification guide, indicating the expected levels of classification.

Limited dissemination v. EUCI

- EU Classified Information (EUCI): any information or material designated by an EU security classification, the unauthorized disclosure of which could cause varying degrees of prejudice to the interests of the EU or of one or more of the Member States.

  RESTREINT UE/EU RESTRICTED

  CONFIDENTIEL UE/EU CONFIDENTIAL

  SECRET UE/EU SECRET

  ~~TRES SECRET UE/EU TOP SECRET~~

- Limited dissemination: access is limited to certain preidentified actors.

Legal framework: Classified information

- Commission Decision 2015/444/EC on the security rules for protecting EU classified information
- Agreements with third countries and international organisations on the exchange of classified information
- National laws

For Horizon 2020 security research projects, the security aspects and the need for classification are assessed by national experts during the security scrutiny.

Security Scrutiny Procedure – SC7 proposals

- **Security Scrutiny Procedure**: after the technical evaluation, SC7 proposals on the main and reserve lists are screened by a group of security experts.

- The **Security Scrutiny Group** consists of national experts nominated by the EU Member States and H2020 Associated Countries. The group is chaired by the European Commission (DG HOME).

- Each proposal is scrutinised by the experts representing the EU Member States and Associated Countries involved in the proposed project.

- The experts use the **Guidelines for the classification of information in research projects** to guide their assessment.

- Applicants receive the result (**Security Scrutiny ESR**) together with the information letter.

Security Scrutiny Results and GAP

- Security Scrutiny Summary Report Format
  - Are there any security concerns? No/Yes, namely.....
  - Are there any security recommendations? No/Yes, namely e.g. nomination of a Project Security Officer, creation of a Security Advisory Board, Limited Dissemination, etc.
  - Will the project use or produce EU classified information?No/Yes, deliverables concerned and classification level

- The outcome of the security scrutiny must be implemented.
- If necessary, section 6 will be revised during the GAP.
- Projects involving EUCI will receive a Security Aspects Letter (SAL) and a Security Classification Guide (SCG) template during the GAP. These become part of the Grant Agreement.

- Optional articles 37.1 (results with a security recommendation) and 37.2 (EUCI) are inserted in the grant agreement.

Security aspects during and after the life of the project

- During the kick-off meeting the project will receive **instructions on the handling of EUCI.** These must be respected at all times.

- **Changes in the classification and/or dissemination level** require the prior written approval of the Commission.

- Information can only be upgraded/downgraded in duly justified cases via an amendment.

- Changes in the **security context** should be immediately notified.

- **Non-compliance** with the security recommendations may lead to reduction or termination of the grant and/or sanctions (Art. 37.4).

- The consortium **remains responsible** for the protection of EU classified information after the end of the project.

How to make your proposal ‘security ready’?

Proposal Preparation 1/2

- Examine if the proposal might raise security issues and/or use or produce classified information. Answer the questions in section 6 accordingly.
    - Check if the WP, call and topic identify specific security risks.
    - Use the Guidelines for Classification of Information in Research Projects to assess if there might be a need to classify certain deliverables (results).
    - Check if classified background information will be used.
- If the project might raise security issues or is expected to involve EUCI, you need to make sure that the consortium has the capacity to deal with these issues.
- Consider appointing a Project Security Officer and/or a Security Advisory Board. Describe the role of the PSO/SAB and indicate who would take on these responsibilities.
- Factors to consider: background, expertise, security clearance, nationality
- Allocate sufficient resources

Proposal Preparation 2/2

- If you are planning to use or produce EU classified information:
  - List all the classified background documents, specify the classification level and the originator giving permission to use the information.
  - List all the deliverables that should be EU classified, specify the classification level and the beneficiaries who will have access to the information. Mark these deliverables also as EU classified in other sections.
  - Indicate which entities and individuals have security clearances.
  - Familiarise yourself with the rules on handling EU classified information.
  - For non-EU partners: check if there is a security agreement between the EU and the country/countries concerned.
  - Do NOT include classified information in your proposal.
- (Personal) data protection is not the same as protecting EUCI.
- Do not copy-paste sections from previous proposals or projects without reassessing the security context.

References

- HORIZON 2020 WORK PROGRAMME 2018-2020 General Annexes, Annex J. Actions involving classified information:

https://ec.europa.eu/research/participants/data/ref/h2020/other/wp/2018-2020/annexes/h2020-wp1820-annex-j-classinfo_en.pdf

- Guidelines for the classification of information in research projects:

https://ec.europa.eu/research/participants/data/ref/h2020/other/hi/secur/h2020-hi-guide-classif_en.pdf

- COMMISSION DECISION (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information:

https://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:32015D0444&from=EN

Thank you!

Any Questions?