



## **EU Grants**

# How to handle security-sensitive projects

Projects with sensitive and classified information

Version 1.0  
01 July 2021



<b>HISTORY OF CHANGES</b>		
<b>Version</b>	<b>Publication Date</b>	<b>Change</b>
1.0	01.07.2021	▪ Initial version (new MFF)
		▪
		▪
		▪
		▪
		▪

## IMPORTANT NOTICE

This guidance is designed to help **applicants and beneficiaries** of **EU projects** get an overview of the additional procedures you need to follow if your project involves security-sensitive or classified information.

It has been prepared mainly for 3 EU Programmes: [Horizon Europe \(HE\)](#), [Digital Europe \(DEP\)](#) and [European Defence Fund \(EDF\)](#). But it can also be used for other programmes that may require a security review to authorise funding (*AMIF, ISF, EU4H, etc*).

The guidance will help you with the security self-assessment at proposal stage and the special security documents you may be asked to fill out during grant preparation. In addition, it contains instructions about the handling of security sensitive projects during grant implementation.

The security self-assessment is part of the security review process that must be conducted by EU granting authorities before they can sign security-sensitive grants. It aims to identify projects that may require EU classification of information (EUCI) under Decision [2015/444](#) and/or other security recommendations.

In this case, your proposal will have to undergo a formal security scrutiny (conducted together with experts who may come from the national security authorities), in order to determine the classification levels that you will need to follow. The specific requirements will be set out in security section containing a Security Aspects Letter (SAL) and a Security Classification Guide (SCG), that will be annexed to your Grant Agreement and thus become part of your grant.

### Further reading

More information on EU classified information can be found in the programme-specific guidance [Classification of information in Horizon Europe projects](#), [Classification of information in Digital Europe projects](#), [Classification of information in EDF projects](#).


**Table of contents**

<b>1. Proposal stage: The Security Issues Table.....</b>	<b>3</b>
<b>2. Grant preparation stage: Part B – Security section, Security Aspects Letter (SAL) and Security Classification Guide (SCG).....</b>	<b>5</b>
<b>3. Project implementation stage .....</b>	<b>6</b>

## 1. Proposal stage: The Security Issues Table

At proposal stage, you will need to fill out the Security Issues Table (either directly in the Submission System or on paper) and, in case of issues, a security self-assessment to explain how the issues will be addressed.

For some [Horizon Europe](#) calls, you will also be asked to already prefill the Part B of the Application Form (*security section with security aspects letter (SAL) and security classification guide (SCG)*), to help us with the security scrutiny.

 Proposals must NOT contain classified information. The Funding & Tenders Portal electronic exchange system cannot be used for classified information.

### 1.1 EUCI and participation of non-EU countries

1. EU classified information (EUCI)		Yes/No	Page
Does the activity involve information and/or materials requiring protection against unauthorised disclosure (EUCI)?			
If YES:	- Is the activity going to use classified information as background information?		
	- Is the activity going to generate EU classified foreground information as results?		
Does the activity involve non-EU countries?			
If YES:	- Do participants from non-EU countries need to have access to EUCI?		
	- Do the non-EU countries concerned have a security of information agreement with the EU		


This section refers to activities that involve classified information, i.e. data or information requiring protection under EU Decision [2015/444](#) and the [Implementing rules on classified grants](#) (or under national rules).

You must reply 'Yes' to the first question of the Security Issues Table if your project is going to involve classified background or foreground information.

**Classified background information** — is any information (documents/deliverables/materials) already classified by an EU institution, EU Member State, non-EU country or international organisation, which is envisaged to be used during and for the purposes of the project.

**EU classified foreground information (EUCI)** — is any information (documents/deliverables/materials) that will be generated as result of the project and which needs to be protected from unauthorised disclosure.

EU classification is normally needed if your 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](#).

 Don't forget that if you intend to use classified background, you must obtain formal written authorisation, in advance, by the originator (*i.e. the authority under whose authority the information was created and classified*).

**Non-EU country participants** — If access to EUCI by participants from non-EU countries is needed for the project (as beneficiaries, affiliated entities, associated partners or subcontractors), this is only possible if the non-EU country where they are established has concluded a security of information agreement with the EU. Otherwise, you will have to attribute the project tasks to another participant (or replace the participant by an entity that can have access to EUCI).

Several non-EU countries have security of information agreements with the EU (see Council document [15035/19](#): *Australia, Bosnia and Herzegovina, Republic of North Macedonia, Iceland, Israel, Liechtenstein, Montenegro, Norway, Serbia, Switzerland, Ukraine, United States of America*).

## 1.2 Misuse

2. Misuse		Yes/No	Page
Does the activity have the potential for misuse of results?			
If YES:	- Does the activity provide knowledge, materials and technologies that could be channelled into crime and/or terrorism?		
	- Could the activity result in the development of chemical, biological, radiological or nuclear (CBRN) weapons and the means for their delivery?		

This section concerns activities involving or generating materials, methods, technologies or knowledge that could be misused for malevolent purposes.

Even if such activities are carried out with benign intentions, they have the potential to have substantial direct impacts on the security of individuals, groups or States. If project activities lead to results whose unauthorised disclosure could prejudice the interests of the EU or its Member States, they must be protected and, when appropriate, classified.

For more information, see the [Guidance note on potential misuse of research](#).


## 1.3 Other security issues

3. Other security issues		Yes/No	Page
Does the activity involve information and/or materials subject to national security restrictions?			
If Yes, please specify (max 1000 characters):			
Are there any other security issues that should be taken into consideration?			
If Yes, please specify (max 1000 characters):			

If your project raises new security issues and concerns that are not covered by the other questions, you should address them in this section.

Such concerns can cover both national security restrictions (other than misuse) and other issues.

In this case, describe the issues and explain how you intend to address them. This allows us to analyse the situation and provide you with appropriate assistance for addressing them. It also avoids the problems you would have if such issues were found out only later (*e.g. in the context of an audit or investigation*).

 Do NOT cover other issues such as ethics, data protection, focus on civil applications etc. They are outside the security review and covered by other parts of the selection procedure (for [Horizon Europe](#), see [guidance note on Research with exclusive focus on civil applications](#)).

## **2. Grant preparation stage: Part B – Security section, Security Aspects Letter (SAL) and Security Classification Guide (SCG)**


### **2.1 Classified information – SAL and SCG**

If the project involves EUCI, you will be requested during grant preparation to add the Security Aspects Letter (SAL) and Security Classification Guide (SCG) to Annex 1 of your Grant Agreement.

The SAL lists the project-specific security requirements linked to the EUCI (*e.g. classification levels, access by consortium-members which are international organisations or entities from non-EU countries, etc*). The SCG describes the classified elements of a grant agreement (deliverables) and their security classification levels (— two separate tables, one for the classified background information and one for the EU classified foreground information).

You must adapt your SAL and SCG to the outcome of the security scrutiny procedure (SecSR).

List all entities that need to know in the SCG (both for classified background and foreground information). Entities not listed there will NOT have access to the classified information listed in the table, even if they are from the project consortium.

 If you will use classified background, don't forget that you must obtain advance formal written authorisation by the originator (*i.e. the entity under whose authority the information was created and classified*).

### **2.2 Other security recommendations**

In addition to the SAL and SCG, you will be requested to complete the information regarding other security recommendations (*e.g. sensitive information with security recommendation, security staff, access to IT systems, etc*).

If your project involves classified background or foreground information, you must appoint a project security officer (PSO). One PSO per project is sufficient. The PSO must have appropriate security clearance.

A security advisory board is needed if your project involves sensitive deliverables with security recommendation or classified background or foreground information.

### 3. Project implementation stage


During project implementation, you must ensure compliance with Decision [2015/444](#), the [Implementing rules on classified grants](#) and the Programme security instructions (PSIs; one per EU Programme):

- [Horizon Europe PSI](#)
- [Digital Europe PSI](#) (*— to be seen if needed*)
- [EDF PSI](#).

During the implementation of the project, the security issues should be managed by the project security officer (PSO) and/or security advisory board.

Sensitive information with security recommendation or EUCI must not be downgraded, declassified or further disseminated, without the prior written consent of the originator (*i.e. the authority under whose authority the information was created and classified*). For EUCI generated by EU projects this is in principle the European Commission.

These rules will imply that you will sometimes need to follow specific instructions by the granting authority (*e.g. for communication, submission of deliverables, etc*).

 Do not forget that the Funding & Tenders Portal electronic exchange system must NOT be used for classified information. Contact your EU Project Officer in case of questions.