#innovacion
#financiacion
#asesoramiento
#internacionalizacion

ESPAÑA PUEDE.

MINISTERIO DE CIENCIA E INNOVACIÓN

CDTI

@CDTIoficial

Security Appraisal Procedure in Horizon Europe proposals

HORIZONTE EUROPA

@HorizonteEuropa

PhD Marina Martínez-Garcia
NCP Cluster-3 Civil Security Horizon Europe
marina.cdti@sost.be

The Security Scrutiny in HE continues basically the same but… there are significant few changes!

Main novelties

- **Legal basis** in HE Regulation (Art. 20): assessing security issues in research proposals is not only a necessity, but also a **legal obligation**!
- Standardised process for **all activities in HE**.
- **Security Self-assessment by the applicants** in the proposal template for all HE proposals.
- Possibility to **flag a topic as security sensitive in the Work Programme** which influences the routing of the process.
- **Full updated set of guidance material.**

Questionnaire in Part-A of ALL HE proposals… as well a dedicated section in Part-B, in case that ANY answer from the questionnarie is "YES".

HORIZON-CL3-2021-FCT-01-02: Lawful interception using new and emerging technologies (5G & beyond, quantum computing and encryption)

Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR 5.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.
Indicative budget	The total indicative budget for the topic is EUR 5.00 million.
Type of Action	Research and Innovation Actions
Eligibility conditions	The conditions are described in General Annex B. The following exceptions apply: The following additional eligibility conditions apply: This topic requires the active involvement, as beneficiaries, of at least 3 Police Authorities[16] from at least 3 different EU Member States or Associated countries. For these participants, applicants must fill in the table "Eligibility information about practitioners" in the application form with all the requested information, following the template provided in the submission IT tool. Some activities, resulting from this topic, may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes.
Technology Readiness Level	Activities are expected to achieve TRL 5-6 by the end of the project – see General Annex B.

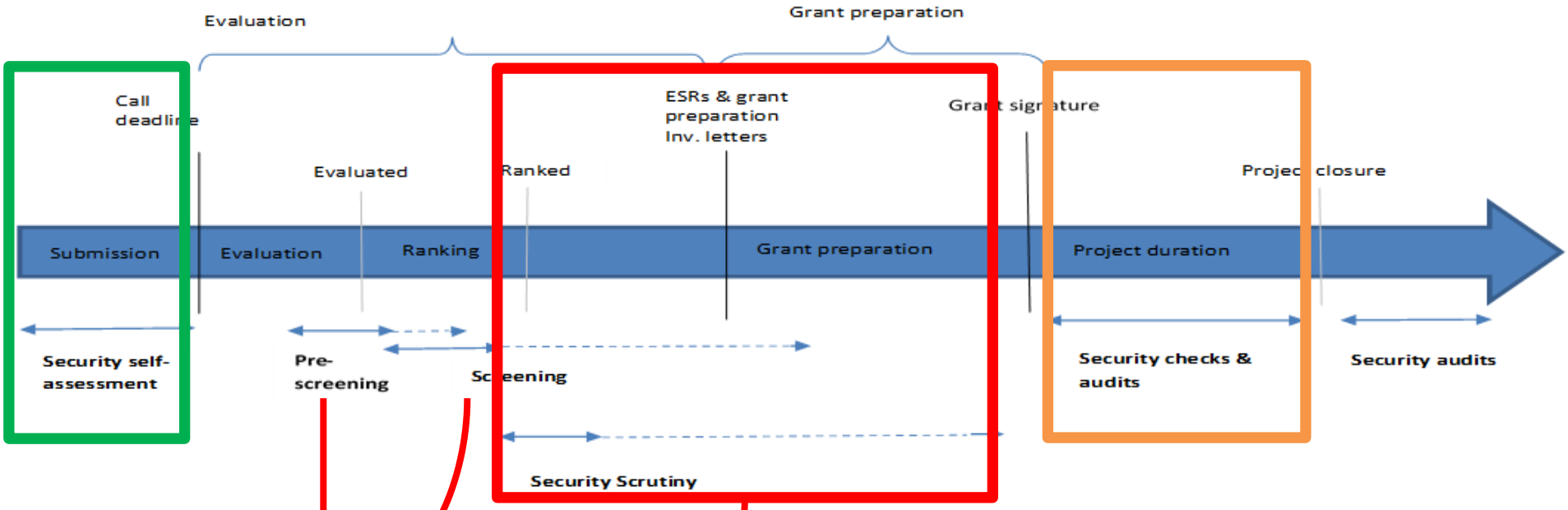
Security Appraisal in HE: overview of the process

The **Security Appraisal Procedure** concerns all activities funded under Horizon Europe and includes **three main steps**:

1. **The Security Self-assessment by the Applicant** – all proposals; → **You must complete part-A & part-B of your proposal!**
2. The **Security Review** by the granting authority, the Commission and national security experts- a selection of proposals; → **For topics in Cluster-3 & topics the Space part of Cluster-4… aswell for any other topic where a potential doubt about security sensitive aspect/research may come out → AFTER THE TECHNICAL EVALUATION and in parallel to the ethical review.**
3. The **Security Checks**, by the Commission or the relevant funding body, where appropriate, during or after the life of the project. → **Checking that all security measure are being taking in place regarding the management of secure sensitive information and deliverables. Modifications in the security classification (up or down) can happened, if considered necessary!**

Possibility to flag a **topic as security sensitive** in the Work Programme influences the routing of the process (**p.e., delays in the GA signature**). At present, the security sensitive topics are from the **Civil Security, ICT related topics (p.e. quantum) and the some space calls.**

En resumen…

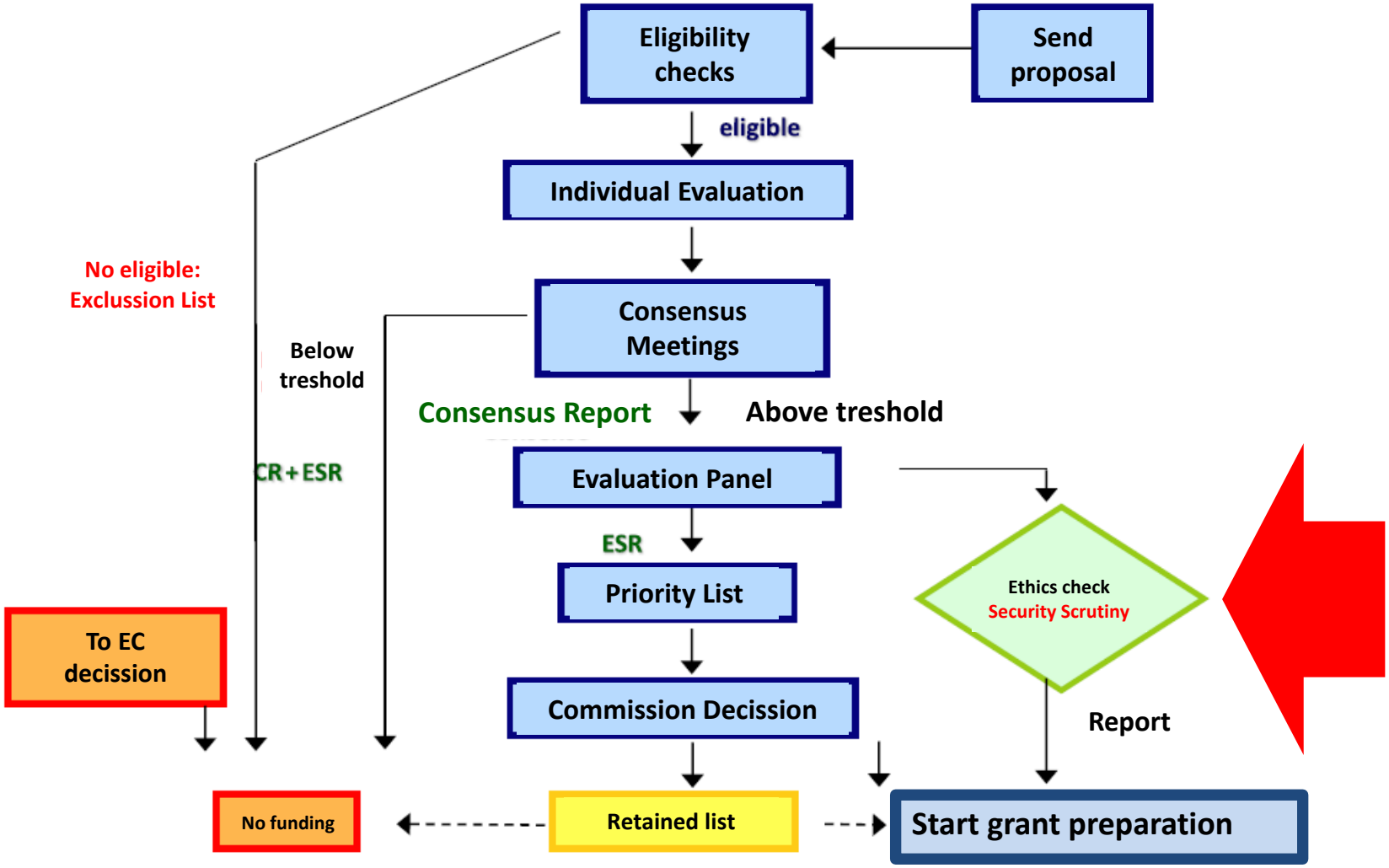


- ✓ **Security Pre-screening:** during the scientific evaluation or soon after- by **granting authority staff**. For proposals submitted under **non- security sensitive topics** when: the **applicant has replied positively** to the Security Issues table or the applicant has replied negatively, but the **granting authority has detected security issues**.

- ✓ **Security Screening:** after the scientific evaluation and before the signature of the GA - by **EC staff** (DG HOME). **Automatically** performed to all proposals that have gone through the Security Pre-screening. DG HOME will assess the pre-screening results and decide on the possible launch of the Security Scrutiny.

1. **Security Scrutiny:** After the scientific evaluation and before the signature of the GA - by **national security experts (Security Scrutiny Group).** → Only **proposals above threshold and considered for funding**, which can lead to **security requirements** that become contractual obligations**. IS NOT A RE-EVALUATION OF THE PROPOSAL AT ALL!.**

Remember the Security Scrutiny…



Overview of the process: Security Self-assessment

The **Security Issues Table (part-A)** includes **3 main questions**:

- **Involvement of information/materials requiring protection against unauthorised disclosure** (classified information) and participation of non-EU countries.
- Potential for **misuse of results**.
- **National security restrictions** or other security issues that should be taken into consideration.

If the answer is "YES" to any of the questions → When preparing a proposal, under a **security sensitive topic**, the applicant is also required to complete a **Security Section in part-B** with more information on specific security issues. Information and guidance can be found in the *Security Section template*.

Attention: The **proposals must not contain** classified information (the IT tool does **NOT** allow applicants to include classified information in a proposal).

Overview of the process: Security Self-assessment

HE proposals will contain a **Security Issues Table, mandatory for all applicants in Part-A.**
Information and guidance can be found in the *How to handle security-sensitive projects*.

Security issues table

Please indicate, by answering Yes or No to all of the questions in the below table, if the proposed activity will use and/or generate information which might raise security concerns. If an answer is Yes, then indicate in the adjacent box at which page in your full proposal further information relating to that issue can be found.

1. EU classified information (EUCI)[2]			Page
Does this activity involve information and/or materials requiring protection against unauthorised disclosure (EUCI)?		○ Yes ○ No	
If **YES**:	Is the activity going to use classified information as background[3] information?	○ Yes ○ No	
	Is the activity going to generate EU classified foreground[4] information as results?	○ Yes ○ No	
Does this activity involve non-EU countries?		○ Yes ○ No	
If **YES**:	Do participants from non-EU countries need to have access to EUCI?	○ Yes ○ No	
	Do the non-EU countries concerned have a security of information agreement with the EU	○ Yes ○ No	
2. MISUSE			Page
Does this activity have the potential for misuse of results?		○ Yes ○ No	
If **YES**:	Does the activity provide knowledge, materials and technologies that could be channelled into crime and/or terrorism?	○ Yes ○ No	
	Could the activity result in the development of chemical, biological, radiological or nuclear (CBRN) weapons and the means for their delivery?	○ Yes ○ No	
3. OTHER SECURITY ISSUES			Page
Does this activity involve information and/or materials subject to national security restrictions?		○ Yes ○ No	
If yes, please specify: *(Maximum number of characters allowed: 1000)*			

Example of a real proposal … in case of answering "YES" in any of the questions in parte-A…

Proposal ID **101070xxx**
Acronym **FANTASTIC**

Security issues table

1. EU Classified Information (EUCI)[2]			Page
Does this activity involve information and/or materials requiring protection against unauthorised disclosure (EUCI)?	(•) Yes	( ) No	14
Is the activity going to use classified information as background[3] information?	( ) Yes	(•) No	
Is the activity going to generate EU classified foreground[4] information as result?	(•) Yes	( ) No	14
Does this activity involve non-EU countries?	(•) Yes	( ) No	1
Do participants from non-EU countries need to have access to EUCI?	(•) Yes	( ) No	1
Do the non-EU countries concerned have a security of information agreement with the EU?	(•) Yes	( ) No	1
2. Misuse			**Page**
Does this activity have the potential for misuse of results?	(•) Yes	( ) No	14
Does the activity provide knowledge, materials and technologies that could be channeled into crime and/or terrorism?	(•) Yes	( ) No	14
Could the activity result in the development of chemical, biological, radiological or nuclear (CBRN) weapons and the means for their delivery?	( ) Yes	(•) No	
3. Other Security Issues			**Page**
Does this activity involve information and/or materials subject to national security restrictions? If yes, please specify: (Maximum number of characters allowed: 1000)	( ) Yes	(•) No	
Are there any other security issues that should be taken into consideration? If yes, please specify: (Maximum number of characters allowed: 1000)	( ) Yes	(•) No	

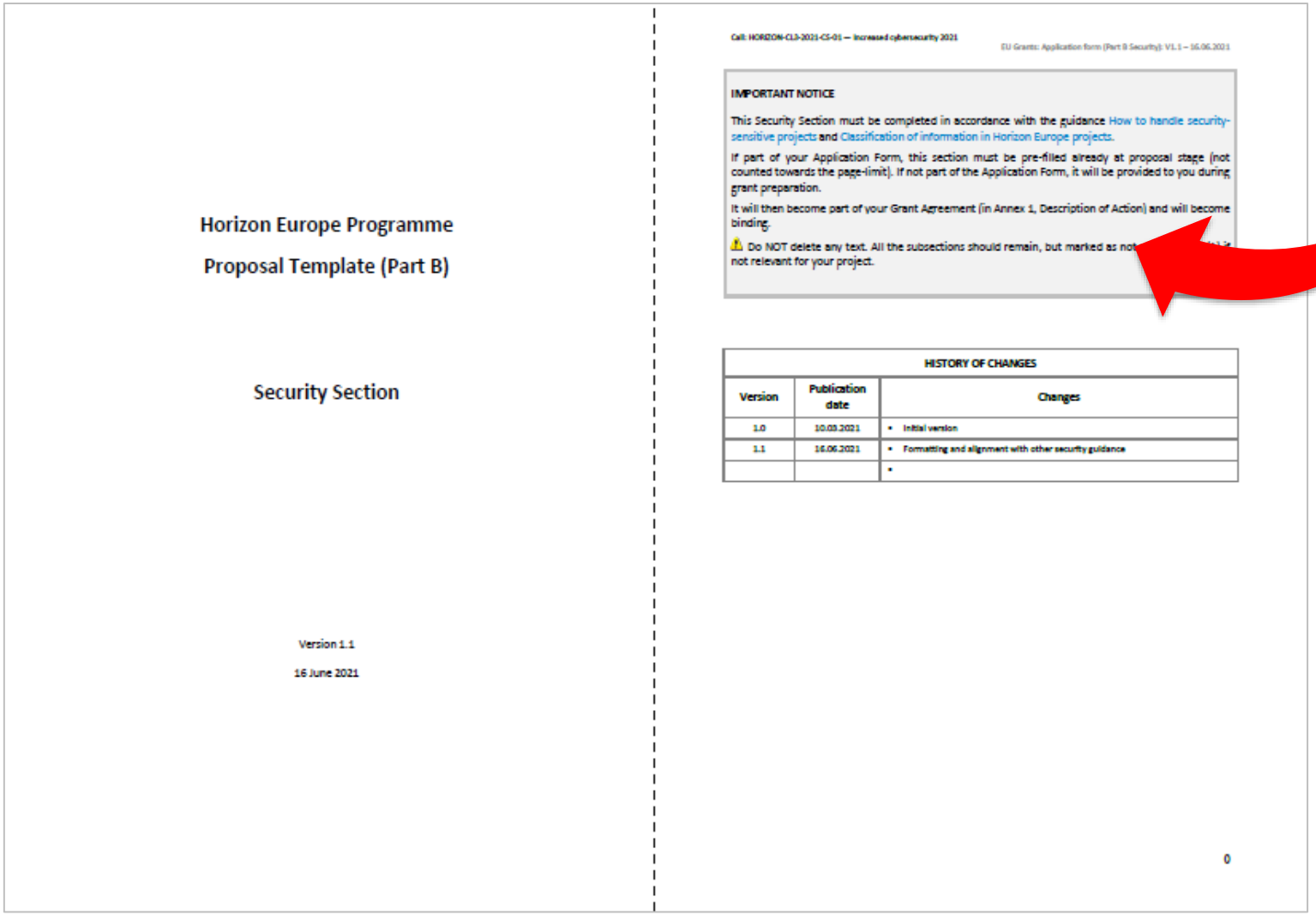
EXAMPLE

[2] According to the Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information, "European Union classified information (EUCI) means any information or material designated by an EU security classification, the unauthorised disclosure of which could cause varying degrees of prejudice to the interests of the European Union or of one or more of the Member States".

[3] Classified background information is information that is already classified by a country and/or international organisation and/or the EU and is going to be used by the project. In this case, the project must have in advance the authorisation from the originator of the classified information, which is the entity (EU institution, EU Member State, third state or international organisation) under whose authority the classified information has been generated.

[4] EU classified foreground information is information (documents/deliverables/materials) planned to be generated by the project and that needs to be protected from unauthorised disclosure. The originator of the EUCI generated by the project is the European Commission.

… Then, you should complete the Security Section en la part-B



Horizon Europe Programme

Proposal Template (Part B)

Security Section

Version 1.1

16 June 2021

Call: HORIZON-CL3-2021-CS-01 — Increased cybersecurity 2021

EU Grants: Application form (Part B Security): V1.1 – 16.06.2021

IMPORTANT NOTICE

This Security Section must be completed in accordance with the guidance How to handle security-sensitive projects and Classification of information in Horizon Europe projects.

If part of your Application Form, this section must be pre-filled already at proposal stage (not counted towards the page-limit). If not part of the Application Form, it will be provided to you during grant preparation.

It will then become part of your Grant Agreement (in Annex 1, Description of Action) and will become binding.

⚠ Do NOT delete any text. All the subsections should remain, but marked as not relevant for your project.

HISTORY OF CHANGES		
Version	**Publication date**	**Changes**
1.0	10.03.2021	• Initial version
1.1	16.06.2021	• Formatting and alignment with other security guidance
		•

0

HORIZONTE EUROPA
@HorizonteEuropa

División de Programas de la UE

ESPAÑA PUEDE.

MINISTERIO DE CIENCIA E INNOVACIÓN

CDTI
@CDTIoficial

… The Security Section in part-B has, basically, 3 sub-sections…

1. Summary of the project security issues

After giving due consideration to Horizon Europe guidance for Security aspects for considering relevant security subject matters, CROSSCON has made the assessment that it will NOT:

a) involve information and/or materials requiring protection against unauthorised disclosure (EUCI);

b) only a swiss partner (CYSEC) is involved from non-EU countries;
c) have the potential for misuse of its results (it will not have activities involving or generating materials, methods, technologies or knowledge that could be misused for malevolent purposes);
d) involve information and/or materials subject to national security restrictions.

There will not be other security issues related to CROSSCON that need to be taken into consideration. For this reason, the following sections are not applicable to CROSSCON.

2. Sensitive information with security recommendation

If your project involves sensitive information requiring limited dissemination due to security reasons, fill in the 'Sensitive information with security recommendation' table below.

- In principle, third parties, i.e. outside the consortium and the granting authority, should have no access to sensitive deliverables with security recommendation.
- However, when it is known in advance that a specific pre-identified group of recipients/recipients with an established need-to-know exists, you should insert them in the table.
- You should conduct an assessment of the recipients' need-to-know, which should be at the disposal of the granting authority, if requested.
- The 'Sensitive information with security recommendation' table may be modified throughout the life of the project. Any **modification can be done only with the prior formal written approval of the granting authority.**
- The table below should not include information that is sensitive for non-security related reasons (e.g. intellectual property or commercial secrets, etc).

Sensitive information with security recommendation			
Number and name of the deliverable	**Name of lead participant**	**Date of production**	**Name of entity authorised for access**

Add as many rows as needed.

Call: HORIZON-CL3-2021-CS-01 — Increased cybersecurity 2021
EU Grants: Application form (Part B Security): V1.1 – 16.06.2021

3. Classified information

3.1 – Security Aspects Letter (SAL)

If your project intends to use or produce classified information, fill in the SAL provided below, according to your project-specific security requirements. Consult the guidance Classification of information in Horizon Europe projects.

- Choose one or more of the Security of Information Agreements with non-EU Countries and/or international organisations, in case beneficiaries from these countries or international organisations participate in the project.
- If relevant, insert in point 6 of the SAL the beneficiaries that must obtain the Facility Security Clearance (FSC) and in point 7, the beneficiaries that must obtain a Personnel Security Clearance (PSC).
- The insertion in the Grant Agreement (Annex 1- Description of Action) of the completed SAL is mandatory, without any modifications on its other parts.

SECURITY ASPECTS LETTER

This security aspects letter (SAL) is an integral part of the classified grant agreement and describes grant agreement specific security requirements. Failure to meet these requirements may constitute sufficient grounds for the grant agreement to be terminated.

The beneficiaries must comply with the minimum standards as laid down in the Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 (hereinafter 'Decision 2015/444') on the security rules for protecting EU classified information, and with its implementing rules.

Without prejudice to Decision 2015/444 and its implementing rules, the beneficiaries should follow the latest version of the Horizon Europe Programme Security Instruction and carry out their responsibilities according to this document.

[If applicable:]

The beneficiaries must also comply with […]

[If relevant, insert one or more of the following Security of Information Agreements with non-EU Countries and/or international organisations]

- The Agreement between Australia and the European Union on the security of classified information signed on 13 January 2010 as attached to the Council Decision 2010/53/CFSP of 30 November 2009, as well as its implementing arrangements.

- The Agreement between Bosnia and Herzegovina and the European Union on security procedures for the exchange of classified information, signed on 05 October 2004, as attached to the Council Decision 2004/731/EC of 26 July 2004, as well as its implementing arrangements.

- The Agreement between the Republic of Iceland and the European Union on security procedures for the exchange of classified information, signed on 12 June 2006, as attached to the Council Decision 2006/467/CFSP of 21 November 2005, as well as its implementing arrangements.

- The Agreement between the European Union and Israel on security procedures for the exchange of classified information, signed on 11 June 2009, as attached to the Council Decision 2009/558/PESC of 16 March 2009, as well as its implementing arrangements.

- The Agreement between the European Union and the Principality of Liechtenstein on security

… The Security Section in part-B has, basically, 3 sub-sections…

impact of incidents associated with the handling and storage of EUCI. The beneficiary or subcontractor must inform the granting authority of its BCP.

3.2 - The Security Classification Guide (SCG) (appendix of the SAL)

If your project intends to use or produce classified information, fill in accordingly the 'Security Classification Guide' tables below. There are two separate SCG tables, one for the classified background information and one for the EU classified foreground information.

- All classified documents (at EU, national or international level) planned to be used by the project should be listed in the SCG for classified background information.
- All EU classified deliverables planned to be produced by the project should be listed in the SCG for EU classified foreground information.
- Different deliverables of the same project can have different classification levels; the same deliverable can be divided in parts, which can be classified at different level.
- Entities (including from the project consortium) not listed in the SCG for both classified background and foreground information should have no access to the classified information listed.
- The SCG for EU classified foreground information may be modified throughout the life of the project. Any modification of the SCG can be done only with the prior formal written approval of the granting authority.
- In case an entity (beneficiary or third party) with an established need-to-know exists, it can be included in advance in the SCG for EU classified foreground information. This entity should be listed as 'reader only'. A detailed description of this entity, their established need-to-know and a reference to Facility Security Clearance, when needed, should be included in the relevant column.

Specific instructions for the table **'Use of classified Background information'**:

Classification Level: mention the existing classification level of the document (EU, national or international classification)

Originator: mention the name of the entity, i.e. EU institution, EU Member State, non-EU country or international organisation, under whose authority the classified information was created and classified

Reference number of the originator's authorisation for the use: you should mention the reference number of the document issued by the originator via which the latter gives authorisation to certain entities of the consortium to use the classified document to be listed in the SCG table. The authorisation letter should be at the disposal of the granting authority, if requested.

Specific instructions for completing the SCG table **'Production of EU classified Foreground information'**:

Classification Level: indicate the classification level proposed by you. In the framework of EU projects, information can be classified as RESTREINT UE/EU RESTRICTED, CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET (grant agreements must not involve information classified TRES SECRET UE/EU TOP SECRET). During grant preparation, update the table with the classification levels fixed in the Security Scrutiny Report.

Responsibility: indicate the role of the entity in relation to the deliverable, e.g. 'Security Manager/Main Contributor', 'Contributor', 'Blind contributor' 'Reader only'. When an entity (beneficiary or third party) is listed as blind contributor, it must have no access to the deliverable.

Call: HORIZON-CL3-2021-CS-01 — Increased cybersecurity 2021
EU Grants: Application form (Part B Security): V1.1 – 16.06.2021

Comments on the need-to-know, purpose of the access and planned use for 'Reader only' role: provide a brief summary of the purpose of the access to the classified deliverable and the planned use. In case an entity (beneficiary or third party) with an established need-to-know exists, it can be included in advance in the SCG. This entity should be listed as 'Reader only'. A detailed description of this entity, its established need-to-know and a reference to Facility Security Clearance, when needed, should be included in this column. The assessment of the entity's need-to-know, should be made available to the granting authority, if requested.

… The Security Section in part-B has, basically, 3 sub-sections…

Security Classification Guide (SCG)			
Use of classified background information			
Reference and name of document	Classification level	Originator (EU institution, EU Member State, non-EU country or IO under whose authority the information was created and classified)	Reference number of originator authorisation for use

Add as many rows as needed.

Security Classification Guide (SCG)					
Production of EU classified foreground information					
Number and name of deliverable	Classification level (R-UE/EU-R, C-UE/EU-C, S-UE/EU-S)	Beneficiaries involved in production / entities authorised for access			
		Name	Responsibility (security manager/main contributor, contributor, blind contributor, reader only)	Date of production	Comments (need-to-know, purpose of access and planned use for 'Reader only' role)

Add as many rows as needed.

4. Security Staff

5. Project Security Officer (PSO)

If your project involves background and/or foreground classified information you should complete the below table. You should also attach a concise CV with the Project Security Officer's relevant security management experience. One PSO appointed per project is sufficient. The PSO should have the appropriate security clearance.

The role of the PSO is to guarantee that the rules on the handling of EU classified information and applicable security procedures are respected.

Project Security Officer		
Name	Nationality	Profession

6. Security Advisory Board (SAB)

If your project involves background and/or foreground classified information you should complete the below table. The SAB should be composed of an uneven number of members (minimum three) consisting of end-user representatives/external reviewer(s) with a good knowledge of the security issues raised by the specific project research field. You should also attach concise CVs describing the SAB members' relevant experience on the security issues in combination with your project's research area. The SAB members should have the appropriate security clearance.

The role of the SAB is to review, throughout the project's life, the project deliverables, in order to assess whether they include any security sensitive information, propose their classification, declassification etc and other timely measures for preventing the misuse of such information.

Security Advisory Board			
Member's name	Nationality	Profession	Areas of competence

Add as many rows as needed.

7. Other project-specific security measures

No additional project-specific security measures

Last considerations regarding the Security Scrutiny…

1. The **Security Scrutiny** will be **carried out in the following cases**:
   - ✓ **Automatically,** when a proposal has been submitted under a **security sensitive topic (Cluster-3 & Space calls from cluster-4)**;
   - ✓ In other cases, when the **Security Screening has concluded that the proposal is very likely to raise security issues** for which mitigation measures should be adopted.

2. The **Security Scrutiny will focus ONLY** on the **potential sensitive information (from the security point of view)** related with your project:
   - ✓ This type of information requires **limited dissemination** due to **security reasons**.
   - ✓ Issues concerning **IPR and commercial secrets fall out of the scope** of this category.
   - ✓ Such information will be marked **as 'SEN' and an additional column will indicate the security type in the deliverables table of part-B** (In H2020 it was marked as Confidential, CO).

3. The **Security Scrutiny** is performed by the the HE Security Security Scrutiny Group of about 58 experts from EU Member State (experts usually working for the National Security Authority or a ministry, e.g. Home Affairs, Security and Justice). → They follow the "**Guidance on Classification of information in Horizon Europe projects**"

But, what can be considered Security Sensitive Information?

Sort of information that can be "Security Sentitive" in your proposal…

It can refers both to the "**subject of research**" as well the "**type of research**" in your project…

Potential sensitive **subject of research:**

- ❑ explosives & CBRN
- ❑ **infrastructure & utilities**
- ❑ border security
- ❑ intelligent surveillance
- ❑ terrorism & organised crime
- ❑ digital security
- ❑ space

Potential sensitive **type of research results (or input information/documents for your project):**

- ❑ threat assessments
- ❑ vulnerability assessments
- ❑ specifications
- ❑ capability assessments
- ❑ incidents/scenarios based on real-life security incidents and potential threat scenarios

… as a consequence, some of the **deliverables**, **activities** or the whole proposal can be secure sensitive classified! → **In Framework Programme projects the common situation in projects is that only deliverables may be classified.**

The best orientation is to use the “Guidance on Classification of information in Horizon Europe projects”

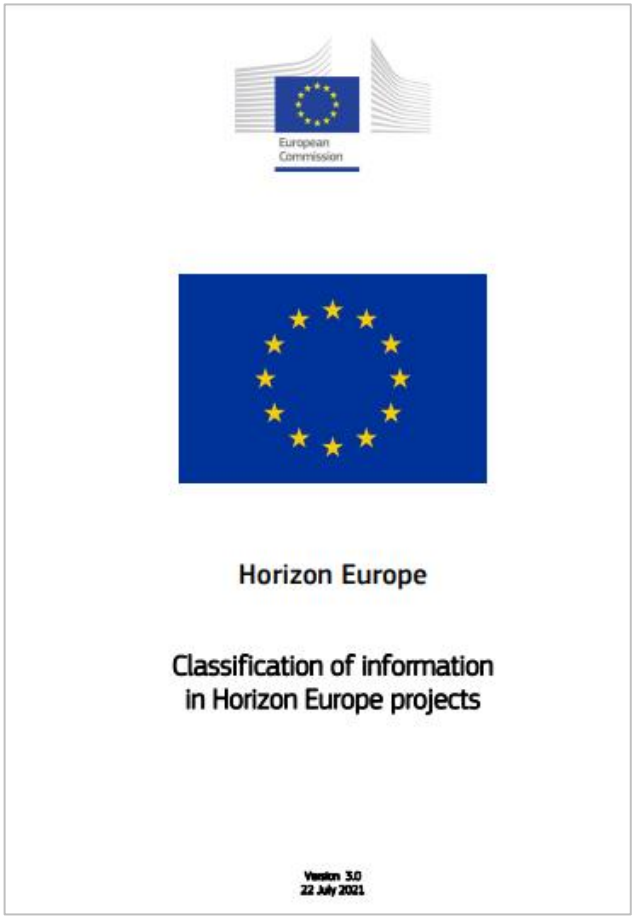


Table of contents

Let’s see the example later on!

https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/classification-of-information-in-he-projects_he_en.pdf

What is considered EU Classified Information (EUCI)?

Classified information (Art. 13.2 MGA and Annex 5) is information requiring protection against unauthorised disclosure.

- A project might **use** classified background information **or produce** classified foreground information.
- **Classified background information → I**s information **already classified by the EU entities, nation states or international organisations,** which is used in the frame of a project.
- **Classified foreground information →** Is information **produced by a project**, which needs to be designated by an EU classification (EUCI).
  - **EUCI definition in Commission Decision 444/2015**: *"European Union classified information (EUCI) means any information or material designated by an EU security classification, the unauthorised disclosure of which could cause varying degrees of prejudice to the interests of the European Union or of one or more of its Member States".*
    - *Example: some of the information produced by a project could potentially be used to plan terrorist attacks or avoid detection of criminal activities.*

Results coming out from the Security Scrutiny of your proposal

- **No security concern** - No security issues were identified in the proposal → No security section in the GA.
- **Security recommendations** - The Security Scrutiny Summary Report (SecScrSR) will list one or more **security requirements** that will be set out in the Security Section of Annex 1 of the GA:
  - security recommendation to **limit the dissemination of sensitive deliverables for security reasons** to the consortium, granting authority staff and potentially to a specific pre-identified group of stakeholders with an established need-to-know;
  - **classification of certain deliverables at a certain level (EUCI);**
  - appointment of a **Project Security Officer (PSO)** in case of classification;
  - establishment of a **Security Advisory Board (SAB)**;
  - **other** security recommendations (e.g. ensuring that personnel has followed trainings on security, adjusting the scope of a certain work package, etc.).

× **Proposal too sensitive to be funded** - information to be used or generated by the project is too sensitive, or applicants lack the right experience, skills or authorisations to handle classified information at the appropriate level. → Funding is refused and the proposal is rejected.

Levels of classification of Security Sensitive Information, EUCI classification

There are **four levels of EU classification of your activities/deliverables**:

- ✓ **TRÈS SECRET UE/EU TOP-SECRET (TS-UE/EU-TS) → ATTENTION:** projects involving information classified TRÈS SECRET UE/EU TOP-SECRET (TS-UE/EU-TS) **cannot be funded under Horizon Europe (as in H2020)**.
- ✓ **SECRET UE/EU SECRET (S-UE/EU-S)**: for information and material the unauthorised disclosure of which **could seriously harm** the essential interests of the European Union or of one or more of the Member States.
  - ✓ *Example: threatening of life or the serious prejudicing of public order or individual security and liberty.*
- ✓ **CONFIDENTIEL UE/EU CONFIDENTIAL (C-UE/EU-C)**: for information and material the unauthorised disclosure of which **could harm** the essential interests of the European Union or of one or more of the Member States.
  - ✓ *Example: inception of damage to the operational effectiveness or security of a Member State or other State's forces or to the effectiveness of valuable security or intelligence operations.*
- ✓ **RESTREINT UE/EU RESTRICTED (R-UE/EU-R)**: for information and material the unauthorised disclosure of which **could be disadvantageous** to the interests of the European Union or of one or more of the Member States.
  - ✓ *Example: information which could potentially make it more difficult to maintain the operational effectiveness or security of Member States or other State's forces.*

Example of the "HE guidelines" regarding a project focus on "Critical Infrastructures"

4.3 Critical infrastructure and utilities research

What?

'**Critical infrastructures and utilities**' are assets and systems *(e.g. buildings and urban areas; energy, water, transport and communications networks; supply chains; financial infrastructures, etc.)* which are essential for maintaining vital social functions *(health, safety, security, economic or social well-being)*[4].

How to deal with threat assessments?

Analyses of man-made threats to infrastructure should be classified RESTREINT UE/EU RESTRICTED. If they add value *(e.g. by prioritising threats)*, they should be classified CONFIDENTIEL UE/EU CONFIDENTIAL.

How to deal with vulnerability assessments?

Detailed gap analyses intrinsic to specific infrastructure and assessments of current security systems, technologies and processes and other extant security solutions should be classified RESTREINT UE/EU RESTRICTED. If they add value *(e.g. by including criticality analyses, highly detailed case studies, vulnerability modelling of supply systems or vulnerability assessment methodologies)* they should be classified CONFIDENTIEL UE/EU CONFIDENTIAL.

Given the specific threat of terrorist attacks on aviation infrastructure, vulnerability analyses of both passenger and cargo security solutions and processes should also be classified CONFIDENTIEL UE/EU CONFIDENTIAL.

How to deal with specifications?

The design, specifications and operation of software tools and platforms to prevent and detect attacks on infrastructure and the design, specifications and operation of architectural security solutions for utilities should be classified RESTREINT UE/EU RESTRICTED.

Detailed detection techniques for early-warning and event analysis *(such as those for use in public transport and urban environments)* and the definition of the data sources to be used should be classified RESTREINT UE/EU RESTRICTED.

Information on sensor networks *(such as those used to identify potential incidents in energy grids, ICT systems or water supply systems)* should be classified RESTREINT UE/EU RESTRICTED. Automated analysis of sensor data, the algorithms used and detailed information on other qualitative and quantitative tools to detect security threats should be classified RESTREINT UE/EU RESTRICTED.

Detailed specifications of organisational and operational processes regarding distribution networks and supply chains *(such as postal systems)* should be classified RESTREINT UE/EU RESTRICTED.

Again, given the higher threat level, the design, specifications and operation of beyond the state-of-the-art screening and detection systems for aviation purposes should be classified CONFIDENTIEL UE/EU CONFIDENTIAL, as should detailed information on airport checkpoint design and procedures. Detailed information on air cargo supply chains should be classified RESTREINT UE/EU RESTRICTED, like other supply chains.

How to deal with capability assessments?

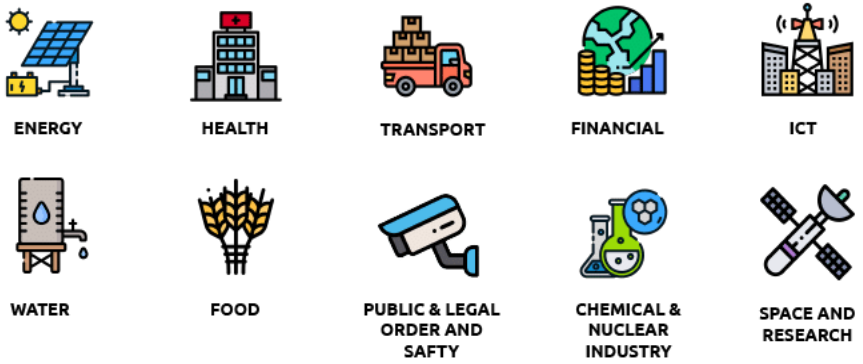
Reports on the performance of systems installed in infrastructure *(such as power plants or water treatment plants)* should be classified CONFIDENTIEL UE/EU CONFIDENTIAL.

The performance of completed detection and security systems in simulated environments *(such as demonstrations of early-warning systems or physical security solutions for buildings)* should be classified RESTREINT UE/EU RESTRICTED.

The capabilities of aviation detection equipment and processes in simulated environments should be classified CONFIDENTIEL UE/EU CONFIDENTIAL.

How to deal with incidents/scenarios assessments?

Detailed information on scenarios and incidents involving attacks on critical infrastructure should be classified RESTREINT UE/EU RESTRICTED. If it adds value *(e.g. by including in-depth quantitative analyses of the potential or actual consequences (human, functional or financial) of such actions)*, it should be classified CONFIDENTIEL UE/EU CONFIDENTIAL.



HORIZONTE EUROPA
@HorizonteEuropa

División de Programas de la UE

ESPAÑA PUEDE.

MINISTERIO DE CIENCIA E INNOVACIÓN
CDTI
@CDTIoficial

Security aspects regards not only the subject but also to “who” may access…

Third Countries & Associated Countries

- EU classification is **limited to EU Member States (EUCI deliverables)**.
- Projects involving classified information can, in principle, include participants from non- EU countries… **HOWEVER, ONLY beneficiaries from countries with a valid Security of Information Agreement with the EU can access and handle classified information used/produced by the project (EUCI deliverables).** → As a consequence:
  - ✓ **There is NO restriction for non-EU countries without Security Agreement** to the participate to projects involving classified information**, AS FAR AS THEY DON'T HAVE ACCESS TO EUCI information.** → **These partners CANNOT access to deliverables/tasks/background information EUCI.**

  - ✓ The non-EU countries possessing a Security Agreement with the EU are to be found in the **Council document 15035/19 (https://data.consilium.europa.eu/doc/document/ST-15035-2019-INIT/en/pdf) → MOST AGREEMENTS ARE STILL UNDER NEGOTIATION!**

Thus, security sensitive information regards not only to the activities & research done, but also to the consortia!!!

EUCI and proposals involving participants from third countries

- General rule: EUCI is limited to EU Member States
- Projects using/producing EUCI can include participants from associated or third countries
- Countries having a security agreement with the EU (Council level) could refer to that security agreement for handling EUCI
- *Special MoU (Memorandum of Understanding) could be agreed between the countries involved in the handling of sensitive information of a project limited to that project*

➢ Participants from associated countries and/or third countries without a Security Agreement with the EU can participate in projects involving/producing EUCI if no access to sensitive information has been foreseen

Situations that we may face in our consortia…

Two exemples of EXCLUSION

1.- OR WELL FROM ALL THE PROPOSAL, that is, this partner from XX-country CANNOT be member of the consortia… → PLEASE, **check eligibility conditions** at topic level…

P.e.: If the topics says that "ONLY entities stablished in MMSS or Associated Countries", then, p.e.,
Switzerland MAY NOT participate in the consorcium BECAUSE IS NOT AN ASSOCIATED COUNTRY.

2.- OR WELL ONLY some DELIVERABLES are EUCI, then, the associated country can be part of the consortium, BUT if they want to have access to them, then that country has to have signed the agreement of exchange EUCI with the EU. → **ATTENTION:** Upto the moment, UK has NOT signed yet the agreement of exchange EUCI with the EU (…among other agreements that are still pending!).

HORIZON-CL3-2022-CS-01-03: Transition towards Quantum-Resistant Cryptography

Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of between EUR 3.50 and 6.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.
Indicative budget	The total indicative budget for the topic is EUR 11.00 million.
Type of Action	Innovation Actions
Eligibility conditions	The conditions are described in General Annex B. The following exceptions apply: In order to achieve the expected outcomes, and safeguard the Union's strategic assets, interests, autonomy, or security, namely cybersecurity in the field of Quantum-Resistant Cryptography, participation is limited to legal entities established in Member States and associated countries.Proposals including legal entities which are not established in these countries will be ineligible. Some activities, resulting from this topic, may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes.
Technology Readiness Level	Activities are expected to achieve TRL 6 by the end of the project – see General Annex B.
Legal and financial set-up of the Grant Agreements	The rules are described in General Annex G. The following exceptions apply: Beneficiaries may provide financial support to third parties in the form of grants. The maximum amount to be granted to each third party is EUR 300 000 to support the expected outcomes of the topic, for example measuring, assessing and standardizing/certifying future-proof cryptography.

Attention with the neighbours which ARE NOT Associated Countries YET!!!!

HORIZONTE EUROPA
@HorizonteEuropa

Last but not least...

Reference documents

- ✓ **Regulation establishing Horizon Europe**: Security (Art. 20)
- ✓ **Model Grant Agreement**: Confidentiality and security (Art. 13 and Annex 5)
- ✓ **Commission Decision (EU, Euratom) 2015/444** of 13 March 2015 on the security rules for protecting EU classified information.
- ✓ **Commission Decision 2021/259** laying down implementing rules on industrial security with regard to classified grants.
- ✓ **Guidelines for Security Experts on the Security Scrutiny Procedure** (coming soon).
- ✓ **Guidance on the 'classification of information in Horizon Europe projects' (July 2021).**
- ✓ **Guidance on 'How to handle Security sensitive projects' (July 2021).**
- ✓ **Horizon Europe Programme Security Instruction (PSI) (Version 1.0, June 2021).**
- ✓ **HE Programme Guide (June 2021).**
- ✓ Guidance note on 'potential misuse of research'.
- ✓ Guidance note on 'research with an exclusive focus on civil applications'.
- ✓ Security section of the HE proposal template, including the template of the Security Aspects Letter (SAL) and its annex (Security Classification Guide (SCG)).

EU Grants

How to handle security-sensitive projects

Projects with sensitive and classified information

Version 1.0
01 July 2021

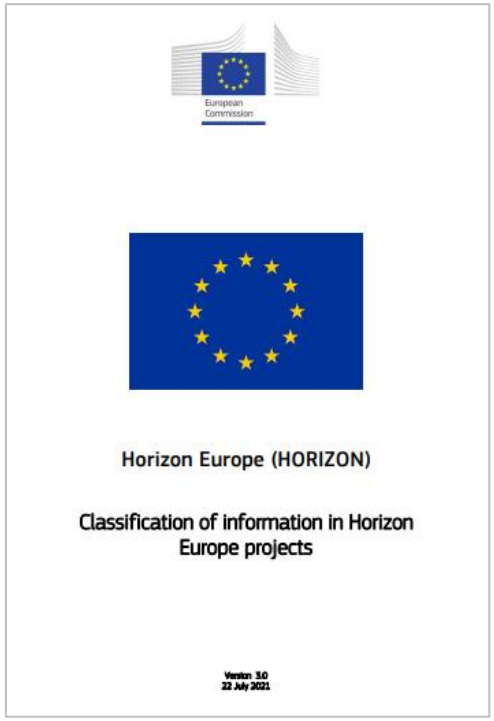
https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/common/guidance/how-to-handle-security-sensitive-projects_en.pdf

HORIZONTE EUROPA
@HorizonteEuropa

División de Programas de la UE

Reference documents

- ✓ **Guidance on the 'classification of information in Horizon Europe projects'** (July 2021).
- ✓ Guidance on **'How to handle Security sensitive projects'** (July 2021).
- ✓ Horizon Europe **Programme Security Instruction** (PSI) (June 2021).



Merci beaucoup!
Dank u wel!

PhD Marina Martínez-Garcia

Framework Programme officer at SOST-CDTI Brussels

Cluster-3 Horizon Europe National Contact Point

marina.cdti@sost.be

HORIZONTE EUROPA @HorizonteEuropa

División de Programas de la UE

ESPAÑA PUEDE.

MINISTERIO DE CIENCIA E INNOVACIÓN

CDTI @CDTIoficial