
HORIZON EUROPE CIVIL SECURITY FOR SOCIETY

SECURITY APPRAISAL



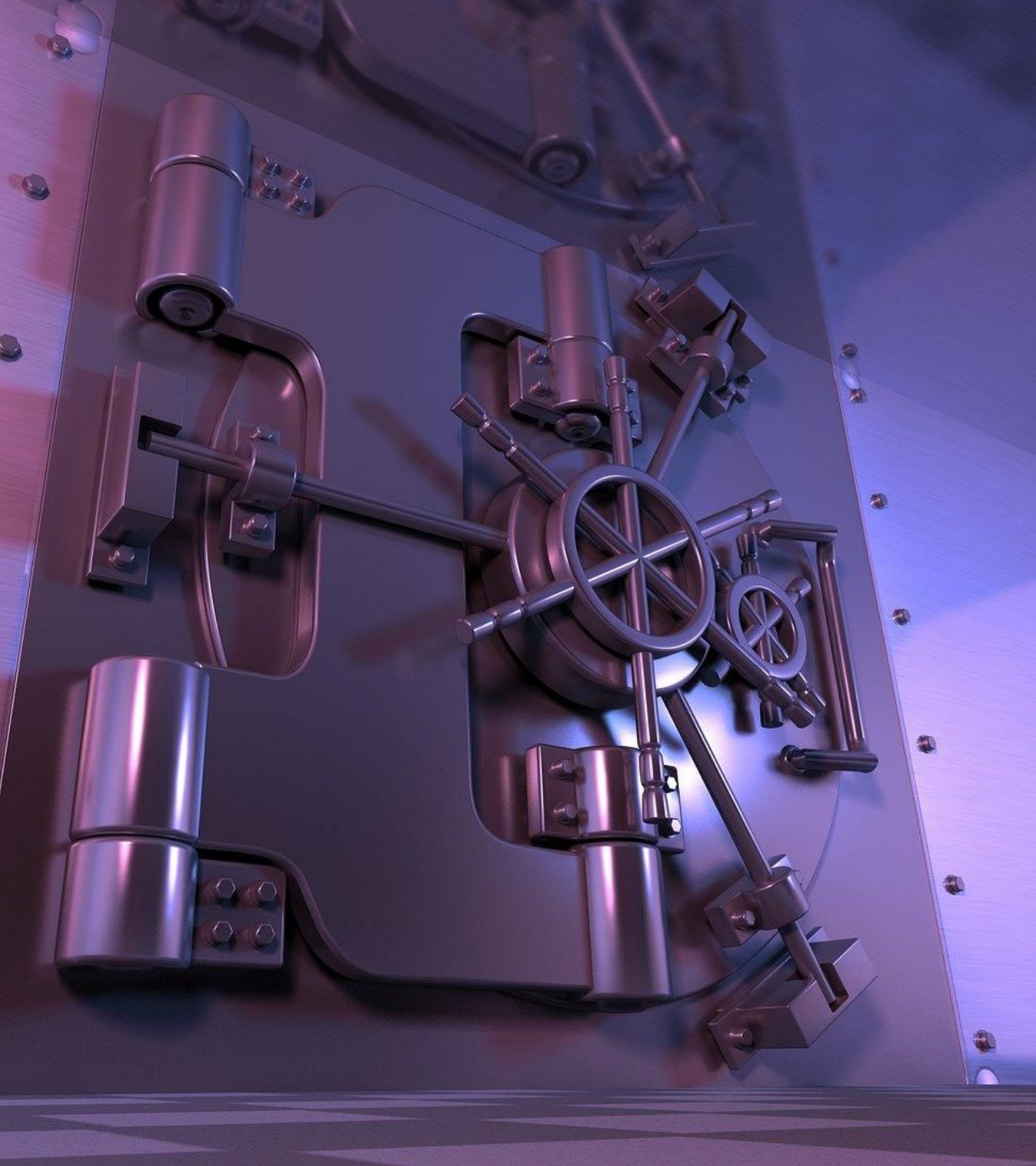
Cluster 3 Info Days
4 March 2026

Blazej Misiak, DG HOME



Overview:

- Why the Security Appraisal is important?
 - Legal basis – art. 20 HE
- How does the process look like?
 - Security self-assessment
 - Security review
 - Outcomes of the Security Scrutiny



Legal basis – art. 20 HE



*Art. 20 (1): “Actions ... shall comply with the applicable security rules and in particular rules on protection of classified information against unauthorised disclosure, including compliance with any relevant **national and Union law.**”*

*Art. 20 (2): “Where appropriate, proposals shall include a **security self-assessment** identifying any security issues and detailing how these issues will be addressed in order to meet the relevant national and Union law.”*

*Art. 20 (3): “Where appropriate, the Commission or funding body shall carry out a **security scrutiny** for proposals raising security issues.”*

What is the Security Scrutiny Procedure (SSP)?

Context

The Security Appraisal aims to identify and address potential **security risks** arising from research activities and prevent **misuse of research** results for criminal or terrorist purposes by implementing effective **mitigation measures**.

Purpose: to assess and address potential misuse of project results (e.g. results that could be channeled into crime or terrorism).

Objectives

- **Identify Security Concerns:** Detect any potential security issues in the proposal.
- **Assess Information Sensitivity:** Determine if sensitive or classified information will be used or generated by the project.
- **Verify Applicant Measures:** Evaluate whether the applicant has adequately addressed identified security issues.
- **Provide Recommendations:** Estipulate solutions to ensure security risks are properly mitigated.



Security Scrutiny Procedure

Flagged Topics

Automatically, if the topic is flagged as 'security sensitive', all projects under that topic will immediately go to security scrutiny (therefore skipping the pre-screening and screening).

| | |
|----------------------------------|---|
| <i>Security Sensitive Topics</i> | 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. |
|----------------------------------|---|

→ The majority of CL3 topics is flagged.

Purpose: to assess and address potential misuse of project results (e.g. results that could be channeled into crime or terrorism).

Non-Flagged Topics

In other cases, if the **Security Screening has concluded that the proposal is likely to raise security issues** for which mitigation measures should be proposed.





Overview of the process

- The Security Appraisal Procedure includes three main steps:
 - The Security **self-assessment** carried out by the applicant,
 - The Security **pre-screening** and **screening** (for non-flagged proposals),
 - The **Security Scrutiny** carried out by the European Commission with support of National Security Experts (**for proposals flagged as security sensitive** and those with positive screening)

Security Appraisal in Horizon Europe



Self-assessment part A – Security Issues Table

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

Security self-assessment

Please specify: (Maximum number of characters allowed: 5000)

Remaining characters 5000

²According 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".

³Classified 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.

- *Security Issues table in the Application form part A is mandatory for all applicants.*
- *Yes/NO questions related to EU Classified Information*
- *YES/NO questions related to misuse of research's results*
- *Other Security Issues*

Additional security section – part B

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.*

*For topics flagged as security sensitive in the Work Programme (the applicant will also have to complete a **mandatory Security Section with more information on specific security issues**). These proposals will go directly to the Security Scrutiny.*

- *Security Aspects Letter (SAL)*
 - *Security of information agreement with non-EU countries*
 - *Facility Security Clearance (FSC)*
 - *Personal Security Clearance (PSC)*
- *Security classification guide (SCG) – background / foreground EUCI*
- *Security Staff (Security Advisory Board, Project Security Officer)*

| Security classification guide (SCG) | | | |
|---|----------------------|--|--|
| Use of classified <u>background</u> 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 for use |
| | | | |
| | | | |

| Production of EU classified <u>foreground</u> 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, blind contributor, reader only) | Date of production | Comments (need-to-know, purpose of access and planned use for 'Reader only' role) |
| | | | | | |

Self-assessment – Security Section Part B

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

| Project security officer (PSO) | | |
|--------------------------------|-------------|------------|
| Name | Nationality | Profession |
| | | |
| | | |

| Security advisory board (SAB) | | | |
|-------------------------------|-------------|------------|---------------------|
| Member's name | Nationality | Profession | Areas of competence |
| | | | |
| | | | |
| | | | |

- *Sensitive information for security reasons must be appropriately identified.*
- *e.g. Information on gaps and vulnerabilities in existing systems or critical infrastructures, requirements used in devices used in detection, law enforcement measures to counter terrorism, etc.*
- *Limited dissemination, limiting the level of detail, using a fake scenario.*
- *The Security Staff such as the Project Security Officer (PSO) and the Security Advisory Board (SAB) must be established in case EU Classified Information is involved.*

How to assess sensitive and classified information?

| Category | Definition |
|----------------------------------|--|
| Public (PU) | Information that is fully open and intended for unrestricted dissemination |
| Sensitive (SEN) | Information that must remain confidential. This category covers commercially sensitive details, trade secrets, confidential data, valuable results awaiting IP protection, or security-sensitive info. |
| Sensitive for security reasons | It is a sub-category of Sensitive. The disclosure is restricted to consortium, Commission, and approved stakeholders with a need to know. Sometimes it is called sensitive non-classified. It requires stricter handling due to potential security implications. |
| EU Classified Information (EUCI) | Information whose unauthorized disclosure could adversely affect EU/MS interests. |
| Classified Background | Information already classified by EU, MS, or international organizations. |
| Classified Foreground | Information produced during project and classified as EUCI. |

Classified deliverables



Restreint UE/EU
Restricted



Confidentiel
UE/EU
Confidential



Secret UE/EU
Secret



Tres secret
UE/EU Top
secret*

* It is too sensitive to be funded
under HE

Classified Deliverables

| Level | Abbreviation | Impact if disclosed | Example |
|------------------------------------|--------------|--|---|
| TRÈS SECRET UE/EU TOP-SECRET | TS-UE/EU-TS | The unauthorized disclosure of this information could cause exceptionally grave harm to the EU and its MS. | Projects TRÈS SECRET UE/EU TOP SECRET cannot be funded under the Horizon Europe Programme |
| SECRET UE/EU SECRET | S-EU/EU-S | Please use this classification for information which could seriously harm essential EU or national interests. | Threatening of life or the serious prejudicing of public order or individual security and liberty. |
| CONFIDENTIEL UE/EU CONFIDENTIAL | C-UE/EU-C | Please use this for information which could harm essential EU or national interests. | 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 | Please use this for information which could be disadvantageous to those interests | Information which could potentially make it more difficult to maintain the operational effectiveness or security of Member States or other State's forces |

Further information

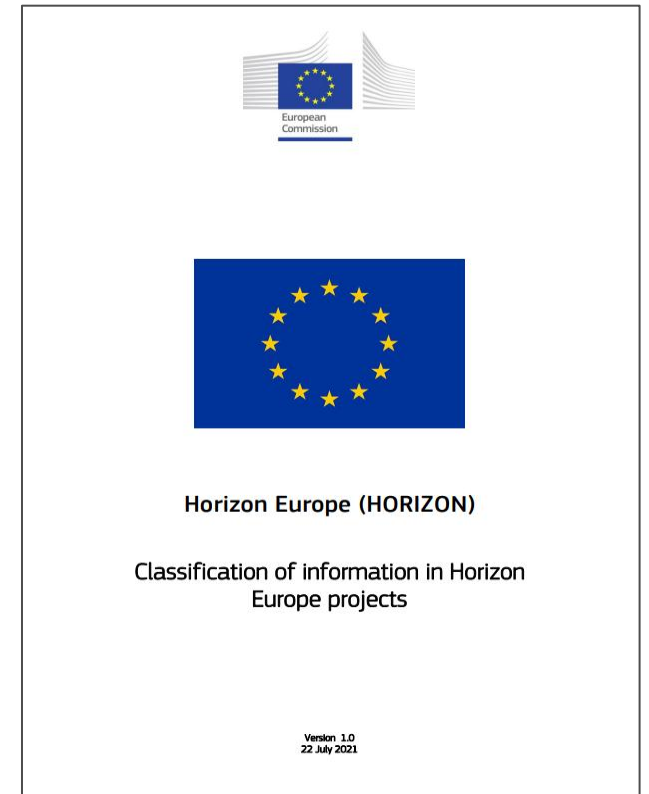


[How to handle security sensitive projects](#)



Watch the **full video on:**

- [Innovation and security research webpage](#)
- [DG Migration and Home affairs Youtube channel](#)



[Classification of information
in Horizon Europe projects](#)



- **No security concern** - No security issues were identified in the proposal.
- **Security recommendations and/or security classification**- The Security Scrutiny Summary Report (SecScrSR) will list one or more **security requirements** that may include:
 - security recommendation to **limit the dissemination level** of certain deliverables for security reasons,
 - **classification** of certain deliverables at a certain level,
 - appointment of a **Project Security Officer (PSO)** in case of classification,
 - establishment of a **Security Advisory Board (SAB)**,
- **Proposal too sensitive to be funded** - The Security Scrutiny may reveal that the information to be used or generated by the project is too sensitive, or that the applicants lack the right experience, skills or authorisations to handle classified information at the appropriate level. In such cases, funding is refused and the proposal is rejected.

Security Recommendations and/or Classification:
outcome of the SSP becomes the Security Section of
Annex 1 of the Grant Agreement (**contractual
obligation**)

Guidance documents available in the EU funds Portal

- [How To Handle Security-Sensitive Projects Guide](#)
- [Guidelines on the Classification of Information in Horizon Europe Projects](#)
- [Horizon Europe Programme Guide](#)
- [Horizon Europe Programme Security Instruction \(PSI\)](#)
- [Guidance note on potential misuse of research](#)
- [Application Form \(Part B Security\)](#)

Legal documents

- [Regulation establishing Horizon Europe](#) (2021/695): Security (Art. 20)
- [HE Model Grant Agreement](#): Confidentiality and security (Art. 13 and Annex 5)
- [Commission Decision 444/2015](#) 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
- [Commission Decision 2019/1961](#) on implementing rules for handling CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information
- [Commission Decision 2019/1962](#) on implementing rules for handling RESTREINT UE/EU RESTRICTED information

Thank you for your attention

In case of questions, please contact HOME-SECURITY-APPRAISAL@ec.europa.eu



© European Union 2020

Unless otherwise noted the reuse of this presentation is authorised under the [CC BY 4.0](https://creativecommons.org/licenses/by/4.0/) license. For any use or reproduction of elements that are not owned by the EU, permission may need to be sought directly from the respective right holders.

Slide xx: [element concerned](#), source: [e.g. Fotolia.com](#); Slide xx: [element concerned](#), source: [e.g. iStock.com](#)

