INFORMATION ON SECURITY ISSUES (SECURITY SECTION)

(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 applicable (N/A) if not relevant for your project.*

⚠ *In order to fill in the template, please consult first the guidance How to handle security-sensitive projects and Classification of information in Horizon Europe projects.*

Summary of the project security issues

Describe the security issues you identified in your project. Focus on the security subject matters and explain the potential misuse of the research results. Relate to the security-sensitive type of activities as explained in the guidance *(see How to handle security-sensitive projects)*.

1. 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.

2. Classified information

2.1 – 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 procedures for exchanging classified information signed on 06 July 2010 as attached to the Council Decision 2010/404/CFSP of 14 June 2010, as well as its implementing arrangements.

- The Agreement between the European Union and Montenegro on security procedures for exchanging and protecting classified information signed on 13 September 2010 as attached to the Council Decision 2010/587/CFSP of 14 June 2010, as well as its implementing arrangements.

- The Agreement between the Republic of North Macedonia and the European Union on security procedures for the exchange of classified information, signed on 25 March 2005, as attached to the Council Decision 2005/296/CFSP, JHA of 24 January 2005, as well as its implementing arrangements.

- The Agreement between the Kingdom of Norway and the European Union on security procedures for the exchange of classified information, signed on 22 November 2004, as attached

to the Council Decision 2004/843/CFSP of 26 July 2004, as well as its implementing arrangements.

- The Agreement between the European Union and the Republic of Serbia on security procedures for exchanging and protecting classified information signed on 26 May 2011 as attached to the Council Decision 2011/514/CFSP of 22 November 2010, as well as its implementing arrangements.

- The Agreement between the European Union and the Swiss Confederation on security procedures for the exchange of classified information, signed on 28 April 2008, as attached to the Council Decision 2008/568/PESC of 24 June 2005, as well as its implementing arrangements.

- The Agreement between the European Union and Ukraine on security procedures for the exchange of classified information, signed on 13 June 2005, as attached to the Council Decision 2005/481/CFSP of 13 June 2005, as well as its implementing arrangements.

- The Agreement between the European Union and the United Kingdom of Great Britain and Northern Ireland concerning security procedures for exchanging and protecting classified information, signed on 30 December 2020, as well as its implementing arrangements[1].

- The Agreement between the European Union and the Government of the United States of America on security procedures for the exchange of classified information, signed on 30 April 2007, as attached to the Council Decision 2007/274/JHA of 23 April 2007, as well as its implementing arrangements.

- The Agreement between the Organisation for Joint Armament Cooperation (OCCAR) and the European Union on the protection of classified information signed on 27 July 2012 as attached to the Council Decision 2012/486/CFSP of 23 July 2012, as well as its implementing arrangements.

- The Agreement between the European Space Agency and the European Union on the security and exchange of classified information signed on 18 July 2008 as attached to the Council Decision 2008/667/JHA of 7 April 2008, as well as its implementing arrangements.

- The Agreement between the European Union and the North Atlantic Treaty Organisation (NATO) on the security of information signed on 14 March 2003 as attached to the Council Decision 2003/211/CFSP of 24 February 2003, as well as its implementing arrangements.

[Information on the above Security of Information Agreements can be found in the Council document 15035/19. Concerning Security Agreements with EU Institutions, Agencies and Bodies, please check with the granting authority].

In particular, but not exclusively, the following security requirements must be complied with:

1. The grant beneficiaries must comply with additional instructions provided by their respective national security authorities (NSAs). If the grant beneficiary faces a problem of application of the applicable legal framework in a Member State, it must refer to the Commission security authority and their NSA or designated security authority (DSA).
2. A list of all the elements to be classified during the performance of this grant agreement as well as the specific applicable security classification levels are contained in the security classification guide (SCG). The SCG is an integral part of this grant agreement and can be found in Appendix to this letter.
3. Classified information generated when performing the grant agreement must be marked as EU classified information (EUCI) at security classification level as determined in the SCG. Deviation from the security classification level stipulated by the SCG is permissible only with the written authorisation of the granting authority.
4. The rights pertaining to the originator of any EUCI created during the performance of the classified grant agreement are exercised by the Commission.
5. Without the written consent of the granting authority, the beneficiary or subcontractor must not make use of any information or material furnished by the granting authority or

[1] This will apply once this Agreement enters into force.

produced on behalf of that authority for any purpose other than that of the grant agreement.

6. A Facility Security Clearance (FSC) is required for the beneficiaries involved in the classified part of the project at the level of CONFIDENTIEL UE/EU CONFIDENTIAL and/or SECRET UE/EU SECRET.

   Where an FSC is required for the performance of a grant agreement, the beneficiary must ask the granting authority to proceed with the FSC request.

   For the performance of this grant agreement, at least the below beneficiaries must obtain the FSC:

   Name of the beneficiary/Abbreviation/Country

   Name of the beneficiary/Abbreviation/Country

   Name of the beneficiary/Abbreviation/Country

7. A Personnel Security Clearance (PSC) is required for the beneficiaries' personnel involved in the classified part of the project at the level of CONFIDENTIEL UE/EU CONFIDENTIAL and/or SECRET UE/EU SECRET.

   Where a PSC is required for the beneficiary's personnel, the beneficiary must directly request its NSA or DSA to initiate the procedure to this effect. The beneficiaries concerned shall maintain records of their employees taking part in the project and who have been cleared for access to EUCI.

   For the performance of this grant agreement, the below beneficiaries must obtain the PSC:

   Name of the beneficiary/Abbreviation/Country

   Name of the beneficiary/Abbreviation/Country

   Name of the beneficiary/Abbreviation/Country

8. The beneficiary or subcontractor must have business contingency plans (BCPs) to protect any EUCI handled in the performance of the classified grant agreement in emergency situations and must put in place preventive and recovery measures to minimise the impact of incidents associated with the handling and storage of EUCI. The beneficiary or subcontractor must inform the granting authority of its BCP.

2.2 - 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.

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.

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.

3. Security Staff

3.1 - 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**

3.2 - 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.

4. Other project-specific security measures

Describe, if relevant, the project security management and other measures intended to safeguard security during the project's life, such as:

- Project staff with a Personnel Security Clearance (PSC) from one organisation without a Facility Security Clearance (FSC) working in the premises of an organisation holding a FSC;
- Specific measures for access to IT systems;
- Other types of measures (technical, operational, etc.)..

HISTORY OF CHANGES		
VERSION	PUBLICATION DATE	CHANGE
1.0	10.03.2021	Initial version (new MFF).
1.1	16.06.2021	Formatting and alignment with other security guidance.
2.0	15.01.2022	Minor reformatting changes and change of document name.