**AGREEMENT BETWEEN**

 **THE GOVERNMENT OF THE REPUBLIC OF SLOVENIA**

 **AND**

**THE GOVERNMENT OF THE REPUBLIC OF MALTA**

**ON**

**THE EXCHANGE AND MUTUAL PROTECTION OF CLASSIFIED INFORMATION**

The Government of the Republic of Slovenia and the Government of the Republic of Malta, hereinafter referred to as the “Parties” and separately as a “Party”,

**ACKNOWLEDGING** the need for effective cooperation in security, military, political, economic and any other area requiring the exchange of Classified Information between the Parties,

**AGREEING** to facilitate contacts between their respective National Security Authorities and Competent Security Authorities,

**COMMITTING** to take all necessary measures to protect the Classified Information transferred, received or created under the terms of this Agreement,

**CONSIDERING** that the Parties mutually recognise the security clearance issued to their own citizens in the area of access to Classified Information,

**AFFIRMING** the respect for the binding rules of international law as well as the national law of the Parties,

**RECOGNISING** the importance of adopting uniform regulations in the area of the protection of Classified Information,

**WISHING** to ensure the protection of Classified Information exchanged between the Parties or between public and private entities under their jurisdiction,

**RESPECTING** the national interests and security of the Parties,

**HAVE AGREED AS FOLLOWS:**

**ARTICLE 1**

**OBJECTIVE AND SCOPE**

(1) The Parties shall, in accordance with their respective laws and regulations, take all appropriate measures to ensure the protection of Classified Information which is transmitted or generated under this Agreement.

(2) This Agreement shall apply to any activities, contract or agreement as well as any other cooperation between the Parties or between legal entities or individuals under their jurisdiction involving Classified Information.

(3) This Agreement may not be invoked by either Party to obtain Classified Information that the other Party has received from a Third Party.

(4) This Agreement shall be in accordance with the national laws and regulations of the Parties.

**ARTICLE 2**

**DEFINITIONS**

For the purposes of this Agreement, the following definitions shall apply:

1. **“Breach of Security”** means any act or omission, which is contrary to the national laws or regulations of a Party, and which leads, or may lead, to disclosure, loss, destruction, misappropriation or any type of compromise of Classified Information;
2. **“Classified Contract”** means a contract or a sub-contract, including pre-contractual negotiations, which contains Classified Information or involves access to such information;
3. **“Classified Information”** means any information, regardless of its form, which is transmitted or generated between the Parties under the national laws or regulations of either Party, and which, in the interests of national security, requires protection against unauthorised disclosure or other compromise, and is designated as such and marked appropriately;
4. **“Competent Security Authority”** means any Designated Security Authority or any other competent entity authorised in accordance with the national laws or regulations of either Party and which is responsible for the implementation of this Agreement;
5. **“Contractor”** means an individual or legal entity possessing the legal capacity to conclude Classified Contracts;
6. **“Facility Security Clearance”** means a determination, following a security clearance process, certifying that a Contractor which is a legal entity fulfils the conditions to handle Classified Information in accordance with the national laws or regulations of the Party concerned;
7. **“Host Party”** means the Party to whose territory a visit pursuant to this Agreement takes place;
8. **“National Security Authority”** means the national authority designated under Article 3 of this Agreement which, in accordance with national laws or regulations, is responsible for the supervision of the implementation of this Agreement and for the control of protection of Classified Information generated or exchanged according to this Agreement;
9. **“Need-to-know”** means the principle by which access to Classified Information may be granted to an individual only in connection with his or her official duties or tasks;
10. **“Originating Party”** means the Party, or any public or private entities under its jurisdiction, which releases Classified Information to the Recipient Party;
11. **“Personnel Security Clearance”** means a determination, following a security clearance process in accordance with national laws or regulations, on the basis of which an individual is authorised to access and handle Classified Information up to the level defined in the security clearance;
12. **“Recipient Party”** means the Party, or any public or private entities under its jurisdiction, which receives Classified Information from the Originating Party;
13. **“Sub-contractor”** means a Contractor to whom a prime Contractor grants a sub-contract;
14. **“Third Party”** means any State, or any public or private entities under its jurisdiction, or an international organisation that is not a Party to this Agreement;
15. **“Transmission”** means conveyance of Classified Information, regardless of its form, between the Parties .

**ARTICLE 3**

**NATIONAL SECURITY AUTHORITIES**

(1) The National Security Authorities designated by the Parties are:

**For the Republic of Malta:**

National Security Authority

Ministry for Home Affairs, Security, Reforms and Equality

**For the Republic of Slovenia:**

The Office of the Government of the Republic of Slovenia for the Protection of Classified Information

(2) The Parties shall notify one another through diplomatic channels of the contact data of their National Security Authorities and of any subsequent changes of their contact data.

(3) The Parties shall notify one another in accordance with Paragraph 3 of the Article 16 of this Agreement as soon as possible, through diplomatic channels, of any subsequent change to their respective National Security Authorities.

(4) The National Security Authorities shall notify one another of any other Competent Security Authorities responsible for the implementation of this Agreement.

(5) The National Security Authorities shall notify one another of the laws or regulations in force in their States, as well as of any changes regarding the protection of Classified Information generated or exchanged in accordance with this Agreement.

(6) In order to achieve and maintain equivalent standards of security, the National Security Authorities may provide one another with information about the security standards, procedures and practises for the protection of Classified Information employed by the respective Party.

**ARTICLE 4**

**SECURITY CLASSIFICATION LEVELS**

(1) Any Classified Information released under this Agreement shall be marked with the appropriate security classification level in accordance with the national laws or regulations of the Parties.

(2) The following security classification levels shall be deemed to be equivalent to one another:

|  |  |  |
| --- | --- | --- |
| **FOR THE REPUBLIC OF MALTA** | **FOR THE REPUBLIC OF SLOVENIA** | **EQUIVALENT IN ENGLISH** |
| L-OGĦLA SEGRETEZZATOP SECRET |  STROGO TAJNO | TOP SECRET |
| SIGRIETSECRET | TAJNO | SECRET |
|  KUNFIDENZJALICONFIDENTIAL | ZAUPNO | CONFIDENTIAL |
| RISTRETTRESTRICTED |  INTERNO | RESTRICTED |

(3) For the Republic of Malta, the Maltese and English markings can be used interchangeably.

(4) The Originating Party may use additional markings indicating special limitations on the use of Classified Information.

(5) The National Security Authorties shall notify one another in accordance with Paragraph 3 of the Article 16 of this Agreement as soon as possible of any amendments to the security classification levels mentioned in Paragraph 2 of this Article.

**ARTICLE 5**

**ACCESS TO CLASSIFIED INFORMATION**

(1) Access to Classified Information shall be limited to individuals who:

a) have a need-to-know;

b) have been briefed on handling and protecting Classified Information; and

c) are duly authorised thereto in accordance with national laws or regulations.

(2) The Parties shall mutually recognise their Personnel Security Clearances and Facility Security Clearances. Paragraph 2 of Article 4 shall apply accordingly.

**ARTICLE 6**

**PROTECTION OF CLASSIFIED INFORMATION**

(1) In accordance with their national laws or regulations, the Parties shall afford to Classified Information under this Agreement the same protection as to their own Classified Information with the corresponding security classification level.

(2) The National Security Authority and/or the Competent Security Authority of the Originating Party shall:

* 1. ensure that Classified Information is marked with an appropriate security classification level in accordance with its national laws or regulations; and
	2. notify the Recipient Party of any conditions of release or limitations on the use of Classified Information, and of any subsequent changes in security classification level.

(3) The National Security Authority and/or the Competent Security Authority of the Recipient Party shall:

1. ensure that Classified Information is marked with an equivalent level of security classification in accordance with paragraph 2 of Article 4; and
2. ensure that the security classification level is not changed without authorisation in writing by the Originating Party.

(4) Each Party shall ensure that appropriate measures are taken to protect Classified Information which is processed, stored or transmitted in communication and information systems. Such measures shall ensure the confidentiality, integrity, availability and, where applicable, the non-repudiation and authenticity of Classified Information, as well as an appropriate level of accountability and traceability of actions in relation to that information.

**ARTICLE 7**

**RESTRICTION ON THE USE OF CLASSIFIED INFORMATION**

(1) The Recipient Party shall use Classified Information solely for the purpose for which it has been released and within the limitations stated by the Originating Party.

(2) The Recipient Party shall not release Classified Information to a Third Party without written consent from the Originating Party.

**ARTICLE 8**

 **TRANSMISSIONOF CLASSIFIED INFORMATION**

1. Classified Information shall be transmitted between the Parties through diplomatic channels. Where such method of transfer proves to be unsuitable or difficult, Classified Information shall be transmitted through other secure channels mutually approved by their National Security Authorities in accordance with national laws or regulations.
2. Classified Information at the RESTRICTED level may also be transmitted by post or another delivery service in accordance with national laws and regulations.

(3) Electronic transmission of Classified Information up to SECRET shall be carried out through certified cryptographic means agreed upon by the Parties.

(4) Where transmitted Classified Information is marked as CONFIDENTIAL or above, the Recipient Party shall confirm its receipt in writing. The receipt of other levels of Classified Information shall be confirmed upon request by the Originating Party.

(5) The transmission of a significant quantity of Classified Information shall be organised between the respective National Security Authorities and/or Competent Security Authorities on a case-by-case basis.

**ARTICLE 9**

**REPRODUCTION, TRANSLATION AND DESTRUCTION OF CLASSIFIED INFORMATION**

(1) All reproductions and translations of Classified Information shall bear appropriate security classification levels and shall be protected in the same way as the original Classified Information. Translations and the number of reproductions shall be limited to the minimum amount required for official purposes.

(2) All translations shall be marked with the security classification level of the original Classified Information, and shall contain suitable annotation in the language of translation indicating that they contain Classified Information of the Originating Party.

(3) Classified Information marked as TOP SECRET as well as its translation shall be reproduced only upon the written consent of the Originating Party.

(4) Classified Information shall be destroyed by the Recipient Party, in accordance with national laws or regulations, when it is no longer considered necessary by the Parties, with the exception of information classified as TOP SECRET which shall be returned to the Originating Party.

(5) Where a crisis situation makes it impossible to protect or return Classified Information transmitted or generated under this Agreement, such Classified Information shall be destroyed immediately and the Recipient Party shall notify the National Security Authority of the Originating Party of such destruction as soon as possible.

**ARTICLE 10**

**CLASSIFIED CONTRACTS**

(1) The National Security Authority and/or the Competent Security Authorities of the Originating Party shall notify the National Security Authority and/or the Competent Security Authorities of the Recipient Party of any Classified Contracts prior to any exchange of Classified Information. Such notification shall specify the highest level of classification of the information involved in the Contract.

(2) A Party that intends to enter into or to authorise one of its Contractors to enter into a Classified Contract with a Contractor of the other Party shall verify with the National Security Authority and/or the Competent Security Authorities of the Recipient Party that the latter has the suitable clearance level required in order to perform the Classified Contract.

(3) Before releasing any Classified Information related to a Classified Contract to Contractors, Sub-contractors or prospective Contractors, the National Security Authority or the Competent Security Authority of the Recipient Party shall:

* 1. ensure that the Contractor, Sub-contractor or prospective Contractor and its facilities are able to provide suitable protection for the Classified Information;
	2. issue the facility an appropriate Facility Security Clearance; and
	3. issue an appropriate Personnel Security Clearance to persons who perform functions which require access to Classified Information.

(4) The Recipient Party shall ensure that all persons having access to Classified Information are informed of their responsibilities and obligations to protect the Classified Information in accordance with national laws or regulations.

(5) The National Security Authority and/or the Competent Security Authority in the territory of the Party in which the Classified Contract is to be performed, shall assume responsibility for prescribing and administering security measures for the Classified Contract under the same standards and requirements that govern the protection of its own Classified Contracts.

(6) The National Security Authority and/or the Competent Security Authority of the Originating Party may request that a security inspection regarding the protection of Classified Information be undertaken at a facility within the Recipient Party’s territory to ensure continuing compliance with security standards in accordance with national laws or regulations.

(7) A Classified Contract shall contain provisions on the security requirements and on the security classification level of each aspect or element of the Classified Contract. A copy of such document shall be submitted to the National Security Authorities and/or the Competent Security Authority of the Parties.

**ARTICLE 11**

**VISITS**

(1) Visits involving access to Classified Information shall be subject to the prior authorisation of the National Security Authority of the Host Party.

(2) Visits involving access to Classified Information shall be allowed only if the visitors have been granted the appropriate Personnel Security Clearance and are authorised to receive or to have access to Classified Information in accordance with their national laws or regulations.

(3) A request for a visit involving access to Classified Information shall be submitted in writing to the relevant National Security Authority and/or to the Competent Security Authority of the Host Party at least three (3) weeks prior to the date of the visit. The request for a visit shall include the following information, which shall be used only for the purpose of the visit:

* 1. the first and last name of the visitor, date and place of birth, nationality and identity card/passport number;
	2. the official capacity of the visitor, with a specification of the entity that the visitor represents;
	3. a specification of the project in which the visitor is a participant;
	4. the validity and classification level of the visitor’s Personnel Security Clearance;
	5. the name, address, phone/fax number, e-mail address and point of contact of the facility to be visited;
	6. the purpose of the visit, including the highest security classification level of Classified Information to be accessed during the visit;
	7. the expected date and duration of the visit;
	8. the date, signature and official seal of the National Security Authority and/or the Competent Security Authority of the Requesting Party; and
	9. other data as may be agreed upon between the National Security Authorities and/or the Competent Security Authority.

(4) In urgent cases, the National Security Authorities and/or Competent Security Authority of the Parties may agree that a request for a visit shall be transmitted in writing at least seven (7) days prior to the date of the visit.

(5) In case of recurring visits, the total period covered by the visits shall be stated in the request for a visit submitted in accordance with paragraph 3 of this Article. The National Security Authorities may agree on a list of visitors entitled to recurring visits, which list shall be valid for an initial period not exceeding twelve (12) months and may be extended for a further period not exceeding twelve (12) months. Once a list of visitors has been approved, visits may be arranged directly between the facilities concerned.

(6) Each Party shall guarantee the protection of personal data and, the health and safety of visitors in accordance with national laws or regulations.

(7) Any Classified Information acquired by a visitor shall be considered as Classified Information under this Agreement.

**ARTICLE 12**

**CO-OPERATION ON THE PROTECTION OF CLASSIFIED INFORMATION**

(1) In order to achieve and maintain comparable standards of security, the National Security Authorities of both Parties shall, upon request, provide one another with information about their national security standards, procedures and practices for the protection of Classified Information, and may visit one another for such purposes.

(2) The National Security Authorities of the Parties shall inform one another of exceptional security risks that may endanger released Classified Information or Classified Information protection systems.

(3) Upon request, the National Security Authorities shall assist one another in carrying out a security clearance process. They shall exchange information on possible security concerns that are of importance in the security clearance process.

(4) The National Security Authorities shall promptly notify one another about any changes in the mutually recognised Personnel Security Clearances and in the mutually recognised Facility Security Clearances.

**ARTICLE 13**

**BREACH OF SECURITY**

(1) In the event of a security breach resulting in the unauthorised disclosure, misappropriation or loss of Classified Information, or a suspicion of such a breach, the National Security Authority of the Recipient Party shall immediately notify the National Security Authority of the Originating Party thereof in writing. Such notice shall contain sufficient detail to enable the Originating Party to fully assess the extent and consequences of the breach.

(2) The National Security Authority of the Recipient Party shall take all appropriate measures under its national laws or regulations to limit the consequences of a breach referred to in paragraph 1 of this Article and to prevent further breaches. Upon request, the Originating Party shall provide appropriate assistance and shall be notified of the outcome of the proceedings and of any corrective measures taken in response to the breach.

(3) Where a breach of security has occurred inside the territory of a Third Party, the National Security Authority of the Recipient Party shall take the measures referred to in paragraphs 1 and 2 of this Article without delay. The Originating Party shall be notified of the results of the investigation and shall receive a report in the English language outlining the causes and extent of the damage.

**ARTICLE 14**

**EXPENSES**

Each Party shall bear its own costs incurred in the course of the implementation and supervision of this Agreement.

**Article 15**

**RESOLUTION OF DISPUTES**

Any dispute regarding the interpretation or application of this Agreement shall be resolved by consultation and negotiation between the Parties and shall not be referred to any international tribunal or Third Party for settlement.

**Article 16**

**Final provisions**

(1) This Agreement shall enter into force on the first day of the second month following the receipt of the last notification with which the Parties notify one another, through diplomatic channels, that their national legal requirements necessary for its entry into force have been fulfilled.

(2) As required, the National Security Authorities and/or the Competent Security Authorities of the Parties shall hold consultations on specific technical aspects relating to the implementation of this Agreement.

(3) This Agreement may be amended by the mutual written consent of the Parties and any such amendments shall form an integral part of this Agreement. Such amendments shall enter into force in accordance with paragraph 1 of this Article.

(4) This Agreement shall be concluded for an indefinite period, and may be terminated by mutual written agreement of the Parties or unilaterally by means of a written notice transmitted through diplomatic channels. In such a case, the validity of this Agreement shall expire six (6) months after the day on which the other Party received notice of termination.

(5) In the event of termination of this Agreement, any Classified Information exchanged pursuant to this Agreement shall continue to be protected in accordance with its provisions and shall, upon request, be returned to the Originating Party.

(6) Additional arrangements may be concluded between the Parties for the implementation of this Agreement.

(7) The Party in whose territory this Agreement is signed shall submit the same Agreement for registration to the Secretariat of the United Nations in accordance with Article 102 of the Charter of the United Nations and shall notify the other Party thereof, including the respective number of the registration.

**IN WITNESS WHEREOF,** the undersigned representatives, being duly authorised by their respective Governments, have signed this Agreement.

**DONE AND SIGNED IN** …………………….on……………………………in two originals, in the Slovenian language and in the English language, both texts being equally authentic.

|  |  |
| --- | --- |
| **For the Government of the Republic of Slovenia**  | **For the Government of the Republic of****Malta**  |