AGREEMENT

BETWEEN

THE GOVERNMENT OF THE REPUBLIC OF MALTA

AND

THE GOVERNMENT OF THE GRAND DUCHY OF LUXEMBOURG

ON MUTUAL PROTECTION AND EXCHANGE OF CLASSIFIED INFORMATION

The Government of the Republic of Malta and the Government of the Grand Duchy of Luxembourg (hereinafter referred to as "the Parties"),

Recognizing that effective co-operation in political, economic, military, security, intelligence and any other area may require exchange of Classified Information between the Parties,

Desiring to establish a system regulating the mutual protection of Classified Information generated or exchanged in the course of the cooperation between the Parties or between public and private entities under their jurisdiction.

Have agreed as follows:

Article 1
Objective and Scope

1.1. The objective of this Agreement is to ensure the protection of Classified Information that is commonly generated or exchanged between the Parties or between public and private entities under their jurisdiction and shall be subject to the applicable national laws of the Parties.

1.2. This Agreement shall apply to any activities, contracts or agreements involving Classified Information that will be conducted or concluded between the Parties following the entering into force of this Agreement.

1.3. The provisions of this Agreement shall also apply to the Classified Information already generated or exchanged in the process of cooperation between the Parties before the entering into force of this Agreement.

Article 2
Definitions

For the purposes of this Agreement:

2.1. "**Breach of Security**" means an act, or omission, contrary to the national laws and regulations, the result of which leads, or may lead, to disclosure, loss, destruction, misappropriation or any other type of compromise of Classified Information;

2.2. "**Classified Contract**" means an agreement between two or more Contractors or Sub-contractors, which contains or involves Classified Information;

2.3. "**Classified Information**" means any information, document or material regardless of its form, which is exchanged or generated between the Parties in accordance with national laws and regulations of either Party, to which a security classification level has been attributed, which requires protection against unauthorized disclosure, misappropriation, loss; or other kind of compromise.

2.4. "**Contractor**" means an individual, or legal entity, possessing the legal capacity to conclude classified contracts;

2.5. "**Facility Security Clearance**" means the determination by the National Security Authority confirming, in accordance with national laws and regulations, that as to whether the Contractor or Sub-contractor meets the conditions for handling Classified Information and up to which security classification level such contractor or sub-contractor shall be allowed to handle;

2.6. "**National Security Authority**" means the national authority, which in accordance with national laws and 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;

2.7. "**Need-to-know**" means the necessity to have access to Classified Information in the scope of given official duties and/or for the performance of a specific task;

2.8. "**Originating Party**" means the Party, including any entity, which provides Classified Information in accordance with national laws and regulations;

2.9. "**Personnel Security Clearance**" means the determination by the National Security Authority confirming, in accordance with national laws and regulations, as to whether an individual is eligible to have access to Classified Information and up to which security classification level such individual shall be eligible to have access to;

2.10. "**Receiving Party**" means the Party, including any entity, to which Classified Information of the Originating Party is transmitted;

2.11. "**Sub-contractor**" means a Contractor to whom a prime Contractor grants a sub-contract;

2.12. **"Third Party"** means any State, including legal entities and individuals under its jurisdiction, or international organization, which is not a party to this agreement.

Article 3
Security Classification Levels

3.1. The Parties undertake to protect Classified Information exchanged between them and agree to adopt the equivalence of the following security classification levels:

For the Republic of Malta	For the Grand Duchy of Luxembourg	English equivalent
L-OGHLA SEGRETEZZA	TRÈS SECRET LUX	TOP SECRET
SIGRIET	SECRET LUX	SECRET
KUNFIDENZJALI	CONFIDENTIEL LUX	CONFIDENTIAL
RISTRETT	RESTREINT LUX	RESTRICTED

3.2. The Originating Party may use additional markings indicating special limitations for use of Classified Information. National Security Authorities shall inform each other in writing of any such additional markings.

Article 4
National Security Authorities

4.1. The National Security Authorities of the Parties are:

For the the Republic of Malta:
National Security Authority
Ministry for Home Affairs and National Security (MHAS)
VALLETTA
MALTA

For the Grand Duchy of Luxembourg:
Service de renseignement de l'État
Autorité nationale de Sécurité
LUXEMBOURG

4.2. The Parties shall notify each other through diplomatic channels on changes of the National Security Authorities. Such notice shall not constitute a formal amendment to this Agreement in accordance with Article 14 paragraph 2.

4.3. The National Security Authorities shall inform each other of the laws and regulations in force in their states, as well as any changes regarding the protection of Classified Information generated or exchanged in accordance with this Agreement.

4.4. In order to achieve and maintain equivalent standards of security, the National Security Authorities may provide each other with information about the security standards, procedures and practises for the protection of Classified Information employed by the respective Party.

Article 5
Measures for the protection of Classified Information

5.1. In accordance with national laws and regulations, the Parties shall take all appropriate measures for the protection of Classified Information, which is exchanged or generated under this Agreement. The same level of protection shall be ensured for such Classified Information of the equivalent security classification levels, as defined in Article 3 of this Agreement.

5.2. The Originating Party shall inform the Receiving Party in writing about any change of the security classification level of the transmitted Classified Information, in order to apply the appropriate protection measures.

5.3. Classified Information shall only be made accessible to individuals who are authorized in accordance with national laws and regulations to have access to Classified Information of the

equivalent security classification level and who have a Need-to-know or are otherwise duly authorised by virtue of their functions, and who have been briefed accordingly.

5.4. For the purposes of this Agreement, each Party shall recognize the Personnel and Facility Security Clearances issued by the other Party.

5.5. The National Security Authorities may assist each other upon request and in accordance with national laws and regulations in carrying out vetting procedures.

5.6. For the purposes of this Agreement, the National Security Authorities shall inform each other without delay about any revocations of Personnel and Facility Security Clearances, or the alteration of the security classification level, as the case may be.

5.7. Upon request of the National Security Authority of the Originating Party, the National Security Authority of the Receiving Party shall issue a written confirmation that an individual has been issued a Personnel Security Clearance or a legal entity has been issued a Facility Security Clearance.

5.8. The Receiving Party shall:

a) not disclose Classified Information to a Third Party without the prior written consent of the Originating Party issued in accordance with national laws and regulations;
b) if deemed appropriate, mark the received Classified Information in accordance with the equivalence set forth in Article 3;
c) not declassify or downgrade the provided Classified Information without the prior written consent of the Originating Party; and
d) use Classified Information only for the purposes that it has been provided for.

Article 6
Transfer of Classified Information

6.1. Classified Information shall be transferred by means of diplomatic or military couriers, or by other means agreed upon in advance by the National Security Authorities, in accordance with national laws and regulations.

6.2. Electronic transmission of Classified Information shall be carried out through certified cryptographic means agreed upon by the Parties.

6.3. If transferred Classified Information is marked SIGRIET / SECRET LUX and above, the Receiving Party shall confirm the receipt in writing. The receipt of other Classified Information shall be confirmed on request.

Article 7
Reproduction and Translation of Classified Information

7.1. Information classified as SIGRIET / SECRET LUX, or above, shall be translated, or reproduced, only in exceptional cases and upon the prior written consent of the Originating Party.

7.2. All reproductions and translations of Classified Information shall be marked with the original markings. Such reproduced or translated information shall be protected in the same way as the original information. The number of reproductions or translations shall be limited to that required for official purposes.

7.3. When making translations and reproductions in accordance with sub-articles (1) and (2), the following procedure shall apply:
(a) the personnel making such translations and reproductions shall be granted the appropriate security clearance; in accordance with their national laws; and
(b) the translations shall clearly indicate in the language of the translation that it contains Classified Information received from the Originating Party.

Article 8
Destruction of Classified Information

8.1. Information classified as L-OGHLA SEGRETEZZA / TRÈS SECRET LUX shall not be destroyed, except in cases referred to in paragraph 4 of this Article. Such Classified Information shall be returned to the Originating Party after it is no longer considered necessary by the Parties.

8.2. Information classified as SIGRIET / SECRET LUX or below shall be destroyed after having been recognized as no longer necessary by the Receiving Party, insofar as to prevent its reconstruction in whole or in part.

8.3. The Receiving Party shall notify the Originating Party about the destruction of information classified as SIGRIET / SECRET LUX.

8.4. In case of a crisis situation, which makes it impossible to protect or return Classified Information generated or exchanged under this Agreement, the Classified Information shall be destroyed immediately. The Receiving Party shall notify the National Security Authorities of both Parties about this destruction as soon as possible.

Article 9
Classified Contracts

9.1. Classified Contracts shall be concluded and implemented in accordance with national laws and regulations.

9.2. Upon request, the National Security Authority of the Receiving Party shall confirm that a proposed Contractor has been issued an appropriate Personnel or Facility Security Clearance. If the proposed Contractor does not hold an appropriate security clearance, the National Security Authority of the Originating Party may request the National Security Authority of the Receiving Party to issue the appropriate security clearance.

9.3. The National Security Authority in which state's territory the Classified Contract is to be performed, shall assume the 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. Periodical security inspections may be carried out by the National Security Authorities.

9.4. A security annex shall be an integral part of each Classified Contract, or sub-contract, by which the Originating Party shall specify which Classified Information is to be released to the Receiving Party, which security classification level has been assigned to that information and the Contractor's obligations to protect the Classified Information. A copy of the security annex shall be sent to the National Security Authority of the Originating Party.

9.5. Prior to release to either Party's Contractors or prospective Contractors of any Classified Information received from the other Party, the Receiving Party shall, in accordance with its national laws and regulations, ensure that Contractors or prospective Contractors can afford adequate security protection to Classified Information and:

a) perform an appropriate Facility Security Clearance procedure of the Contractors and Sub-contractors;

b) perform an appropriate Personnel Security Clearance procedure for all personnel whose duties require access to Classified Information;

c) ensure that all persons having access to Classified Information are informed of their responsibilities;

d) carry out periodic security inspections of relevant security-cleared facilities.

9.6. Sub-contractors engaged in Classified Contracts shall comply with the security requirements applied to the Contractors.

9.7. Visits can be arranged between the National Security Authorities in order to analyze the efficiency of the measures adopted by a Contractor for the protection of Classified Information involved in a Classified Contract.

Article 10
Visits

10.1. Visits that require access to Classified Information shall be subject to the prior written consent by the National Security Authority of the host Party.

10.2. The request for visit shall be submitted at least three (3) weeks prior to the visit and shall contain:

a) visitor's name and surname, date and place of birth, nationality;
b) passport number or another identification card number of the visitor;
c) position of the visitor and name of the organization represented;
d) level of the Personnel Security Clearance of the visitor, if applicable;
e) purpose, proposed working program and planned date of the visit;
f) names of organizations and facilities requested to be visited;
g) number of visits and period required;
h) other data, agreed upon by the National Security Authorities.

10.3. Each Party shall guarantee the protection of personal data of the visitors in accordance with national laws and regulations.

Article 11
Breach of Security

11.1. The National Security Authority of the Receiving Party shall immediately notify the National Security Authority of the Originating Party of any suspicion or discovery of a Breach of Security.

11.2. The National Security Authority of the Receiving Party shall undertake all possible appropriate measures in accordance with its national laws and regulations so as to limit the consequences of the Breach of Security and to prevent further violations and ensure the appropriate investigation. On request, the National Security Authority of the Originating Party shall provide investigative assistance. The National Security Authority of the Receiving Party shall inform the National Security Authority of the Originating Party of the outcome of the proceedings and the corrective measures undertaken due to the violation.

Article 12
Costs

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

Article 13
Settlement of Disputes

Any dispute regarding the interpretation or application of this Agreement shall be settled exclusively by consultations and negotiations between the Parties. The Parties agree that disputes shall not be referred to any national or international tribunal or court or to any third party for settlement. Meanwhile, the Parties will continue to fulfil the provisions set forth in this Agreement.

Article 14
Final Provisions

14.1. This Agreement shall enter into force on the first day of the second month after the date of the receipt of the latest written notification by which the Parties have notified each other, through diplomatic channels, that their national legal requirements necessary for its entry into force have been fulfilled.
14.2. This Agreement may be amended by mutual written consent of the Parties. The amendments shall form an integral part of this Agreement. Such amendments shall enter into force in accordance with the provision of paragraph 1 of this Article.
14.3. This Agreement is being concluded for an indefinite period of time. Either Party may terminate this Agreement by giving the other Party written notice through diplomatic channels. In that case, termination shall take effect six (6) months from the date on which the other Party has received the notice.
14.4. In case of termination of this Agreement, all Classified Information exchanged pursuant to this Agreement shall continue to be protected in accordance with the provisions set forth herein and, upon request, returned to the Originating Party.

Done at New York on 26 September 2019 in two originals, each in the English and French languages, all texts being equally authentic. In case of any divergence of interpretation, the English text shall prevail.

FOR THE GOVERNMENT OF THE REPUBLIC OF MALTA	FOR THE GOVERNMENT OF THE GRAND DUCHY OF LUXEMBOURG
Carmelo Abela	Jean Asselborn
Minister of Foreign Affairs and Trade Promotion	Minister of Foreign and European Affairs