

AGREEMENT

BETWEEN

**THE GOVERNMENT OF
THE REPUBLIC
OF LITHUANIA**

AND

**THE GOVERNMENT OF
THE HELLENIC REPUBLIC**

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

The Government of the Republic of Lithuania

and

the Government of the Hellenic Republic

Hereinafter collectively referred to as the “Parties” and individually as the “Party”,

Wishing to ensure the protection of Classified Information generated or exchanged in the course of cooperation between the Parties or between public and private entities under their jurisdiction,

In respect of the national interests and security of the Parties,

Have agreed as follows (hereafter the “Agreement”):

ARTICLE 1 OBJECTIVE AND SCOPE

- 1.1 The Parties and public and private entities under their jurisdiction shall, in accordance with the Parties’ respective laws and regulations, take all appropriate measures to ensure the protection of Classified Information which is generated or exchanged under this Agreement.
- 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 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, the following definitions shall apply:

Breach of Security: an act or an omission, contrary to the Parties’ respective laws and regulations, which results, or may result in disclosure, loss, destruction, misappropriation or any other type of compromise of Classified Information;

Classified Contract: a contract or a subcontract, including pre-contractual negotiations, which contains Classified Information or involves access to such information;

Classified Information: any information, regardless of its form, which is generated or exchanged between the Parties or between public and private entities under their jurisdiction, under the national laws and regulations of either Party, and which, in the interests of national security, requires protection against unauthorised disclosure, loss, destruction, or misappropriation or any other kind of compromise and is designated as such and marked appropriately;

Contractor: an individual or legal entity possessing the legal capacity to conclude Classified Contracts;

Facility Security Clearance: a determination, following a security vetting process, certifying that a contractor which is a legal entity fulfills the conditions to handle Classified Information of a specified security classification level in accordance with the Parties' respective laws and regulations;

Need-to-Know: a principle by which access to Classified Information may be granted to an individual only in connection with his/her official duties or tasks;

Originating Party: the Party, including any public or private entities under its jurisdiction, which releases Classified Information to the Recipient Party;

Personnel Security Clearance: a determination, following a security vetting process, in accordance with the Parties' respective laws and regulations, on the basis of which an individual is authorised to access to and handle Classified Information up to the level defined in the clearance;

Recipient Party: the Party, including any public or private entities under its jurisdiction, which receives Classified Information from the Originating Party;

Third Party: any State, including any public or private entity under its jurisdiction, or any international organisation that is not a Party to this Agreement.

ARTICLE 3

COMPETENT SECURITY AUTHORITIES

3.1 The National Security Authorities designated in accordance with the Parties' respective laws and regulations by them as responsible for the general implementation of this Agreement and for the assurance of protection of Classified Information generated or exchanged according to this Agreement are:

For the Republic of Lithuania:
Commission for Secrets Protection Coordination,

For the Hellenic Republic:
National Security Authority (NSA), Hellenic National Defence General Staff (HNDGS), Joint Military Intelligence Division (JMID).

3.2 The National Security Authorities shall notify each other in writing of any other competent security authorities responsible for the implementation of this Agreement.

- 3.3 The Parties shall notify each other, through diplomatic channels, of any subsequent changes to their respective National Security Authorities as well as of any change in their respective laws and regulations related to Classified Information.

ARTICLE 4

SECURITY CLASSIFICATION LEVELS

- 4.1 Any Classified Information released under this Agreement shall be marked with the appropriate security classification level in accordance with the Parties' respective laws and regulations.
- 4.2 The Parties undertake to protect Classified Information exchanged between them and agree that the following security classification levels shall be equivalent:

FOR THE REPUBLIC OF LITHUANIA	FOR THE HELLENIC REPUBLIC	IN THE ENGLISH LANGUAGE*
VISIŠKAI SLAPTAI	ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ	TOP SECRET
SLAPTAI	ΑΠΟΡΡΗΤΟ	SECRET
KONFIDENCIALIAI	ΕΜΠΙΣΤΕΥΤΙΚΟ	CONFIDENTIAL
RIBOTO NAUDOJIMO	ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ	RESTRICTED

* Used only for understanding purposes, not for official use.

ARTICLE 5

ACCESS TO CLASSIFIED INFORMATION

- 5.1 Access to Classified Information shall be limited to individuals on a Need-to-Know basis, who have been briefed on handling and protecting Classified Information, and who are duly authorised thereto in accordance with the Parties' respective laws and regulations.
- 5.2 The Parties shall mutually recognise their Personnel Security Clearances and Facility Security Clearances granted in accordance with their respective laws and regulations. Article 4, paragraph 2 of this Agreement, shall apply accordingly.

ARTICLE 6

PROTECTION OF CLASSIFIED INFORMATION

- 6.1 In accordance with their national laws and regulations, the Parties shall take all appropriate measures for the protection of Classified Information, which is generated or exchanged under this Agreement. 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.
- 6.2 The Originating Party shall:

- a) ensure that Classified Information is marked with an appropriate security classification level in accordance with its national laws and regulations, and
- b) inform the Recipient Party of any conditions of release or limitations on the use of Classified Information, and inform in writing of any subsequent changes in security classification level.

6.3 The Recipient Party shall:

- a) in accordance with its national laws and regulations, ensure that Classified Information is marked with an equivalent level of security classification in accordance with Article 4, paragraph 2 of this Agreement, and
- b) ensure that the security classification level is not changed without the prior written consent of the Originating Party.

6.4 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, 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

- 7.1 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.
- 7.2 The Recipient Party shall not release Classified Information to a Third Party without the prior written consent of the Originating Party.

ARTICLE 8 TRANSFER OF CLASSIFIED INFORMATION

- 8.1 Classified Information shall be transferred between the Parties through diplomatic channels or through other secure channels mutually agreed upon in advance by their National Security Authorities in accordance with the Parties' respective laws and regulations.
- 8.2 Information classified KONFIDENCIALIAI/ΕΜΠΙΣΤΕΥΤΙΚΟ and above shall be registered.
- 8.3 Electronic transmission of Classified Information shall be carried out through certified cryptographic means agreed upon by the National Security Authorities.

- 8.4 Classified Information marked as RIBOTO NAUDOJIMO/ΠΕΠΙΟΠΙΣΜΕΝΗΣ ΧΡΗΣΗΣ may also be transferred by post or another delivery service in accordance with the Parties' respective laws and regulations.

ARTICLE 9 REPRODUCTION, TRANSLATION AND DESTRUCTION OF CLASSIFIED INFORMATION

- 9.1 All reproductions and translations 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.
- 9.2 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.
- 9.3 Classified Information marked as VISIŠKAI SLAPTAI/AKPΩΣ ΑΠΟΡΡΗΤΟ, both the original and translation, shall be reproduced or translated only upon prior written consent of the Originating Party.
- 9.4 Classified Information marked as VISIŠKAI SLAPTAI/AKPΩΣ ΑΠΟΡΡΗΤΟ shall not be destroyed. When no longer required, it shall be returned to the Originating Party.
- 9.5 Classified Information marked as SLAPTAI/ΑΠΟΡΡΗΤΟ or below shall be destroyed when it is no longer considered necessary by the Recipient Party, insofar as to prevent its reconstruction in whole or in part, in accordance with its national laws and regulations.
- 9.6 If a crisis situation makes it impossible to protect or return Classified Information generated or exchanged under this Agreement, the Classified Information shall be destroyed immediately. The Recipient Party shall notify the National Security Authority of the Originating Party of its destruction as soon as possible.

ARTICLE 10 CLASSIFIED CONTRACTS

- 10.1 A security annex shall be an integral part of each Classified Contract, or subcontract, by which the contracting authority under the jurisdiction of the Originating Party shall specify which Classified Information is to be released to the Contractor under the jurisdiction of the Recipient 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 Recipient Party.
- 10.2 The National Security Authority of the Recipient Party shall ensure that Classified Information related to a Classified Contract is released to Contractors, subcontractors or prospective contractors after:

- a) it has been ensured that the Contractor, subcontractor or prospective contractor and its facilities are able to provide suitable protection for the Classified Information;
 - b) the facilities have an appropriate Facility Security Clearance; and
 - c) persons who perform functions which require access to Classified Information have appropriate Personnel Security Clearance.
- 10.3 The Recipient Party shall ensure that all persons having access to Classified Information are informed of their responsibilities and obligation to protect the Classified Information in accordance with its national laws and regulations.
- 10.4 The National Security Authority of the Originating Party may request that a security inspection regarding the protection of Classified Information is undertaken at a facility to ensure the continuing compliance with security standards in accordance with its laws and regulations.

ARTICLE 11

VISITS

- 11.1 Visits requiring access to Classified Information shall be subject to the prior authorisation of the National Security Authority of the host Party.
- 11.2 A request for visit shall be submitted to the competent National Security Authority at least three (3) weeks prior to the commencement of the visit. The request for visit shall include for each visitor/participant, the following information, which shall be used only for the purpose of the visit:
- a) first and last name(s) of the visitor, date and place of birth, nationality(ies) and identity card/passport number;
 - b) position of the visitor and name of the organization represented;
 - c) a specification of the project in which the visitor is a participant;
 - d) the validity and classification level of the visitor's Personnel Security Clearance, if required;
 - e) name, address, phone number, e-mail address and point of contact of the facility to be visited;
 - f) the purpose of the visit, including the highest security classification level of Classified Information to be involved;
 - g) the date and duration of the visit, and in the case of recurring visits, the total period covered by the visits shall be stated;
 - h) date and signature of the sending National Security Authority;

- i) other additional data, agreed upon by the National Security Authorities.
- 11.3 In urgent cases, the National Security Authorities may agree on a shorter period for the submission of a request for visit.
- 11.4 The National Security Authorities may agree on a list of visitors entitled to recurring visits. The 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. The request for recurring visits shall be submitted in accordance with the procedure set forth in the second paragraph of this article. Once a list has been approved, visits may be arranged directly between the facilities involved.
- 11.5 Each Party shall guarantee the protection of personal data of visitors in accordance with its national laws and regulations.
- 11.6 Any Classified Information to which a visitor had access to, during his visit, shall be considered as Classified Information under this Agreement.

ARTICLE 12

COOPERATION ON THE PROTECTION OF CLASSIFIED INFORMATION

- 12.1 In order to achieve and maintain comparable standards of security, the National Security Authorities shall, on request, provide each other with information about their national security standards, procedures and practices for the protection of Classified Information.
- 12.2 Upon request, the National Security Authority or any other competent security authority of the Originating Party shall be authorized to visit the other Party in order to ascertain with the National Security Authority or any competent security authority of the Recipient Party, whether the Classified Information exchanged pursuant to this Agreement is protected in accordance with this Agreement.
- 12.3 The competent security authorities shall inform each other of exceptional security risks that may endanger released Classified Information or Classified Information protection systems.
- 12.4 Upon request, and in accordance with the Parties' respective laws and regulations, the National Security Authorities shall assist each other in carrying out a security vetting process. They shall exchange information on possible security concerns that are of importance in the security vetting process.
- 12.5 Upon request of the National Security Authority of the Originating Party, the National Security Authority of the Recipient 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.
- 12.6 The National Security Authorities shall promptly inform each other about any changes in Personnel Security Clearances and Facility Security Clearances.

ARTICLE 13 BREACH OF SECURITY

- 13.1 In the event of a Breach of Security resulting in the unauthorised disclosure, misappropriation or loss of Classified Information or 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 and ensure the initiation of an appropriate investigation.
- 13.2 The competent authorities of the Recipient Party shall take all appropriate measures under its national laws and regulations to limit the consequences of the breach referred to in the first paragraph of this article and to prevent any further breaches. Upon request, the Originating Party shall provide appropriate assistance; it shall be informed of the outcome of the investigation and the corrective measures taken due to the breach.
- 13.3 When a Breach of Security has occurred in a Third Party, the National Security Authority of the Third Party shall be requested by the National Security Authority of the Recipient Party to take without delay the measures referred to in the second paragraph of this article.

ARTICLE 14 EXPENSES

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

ARTICLE 15 RESOLUTION OF DISPUTES

Any dispute regarding the interpretation or implementation of this Agreement shall be settled by consultation and/or negotiation between the Parties and shall not be referred to any national or international tribunal or to any third party for settlement.

ARTICLE 16 FINAL PROVISIONS

- 16.1 This Agreement shall enter into force on the first day of the second month following the receipt of the last notification by which the Parties inform each other, through diplomatic channels, that the internal legal requirements for its entry into force have been fulfilled.
- 16.2 This Agreement may be amended by the mutual, written consent of the Parties. Such amendments shall enter into force in accordance with the procedure set forth in the first paragraph of this article.

- 16.3 This Agreement shall be concluded for an indefinite period. Either Party may terminate this Agreement by giving a written notice of termination to the other Party through diplomatic channels. In such case, this Agreement will be terminated six (6) months after the date of the receipt of the termination notice by the other Party.
- 16.4 In the event of termination of this Agreement, any Classified Information exchanged or generated under this Agreement shall continue to be protected in accordance with the provisions set forth herein and, upon request, returned to the Originating Party.
- 16.5 Where necessary, the National Security Authorities or any other competent security authorities of the Parties may consult each other on detailed technical aspects relating to the application of this Agreement and may conclude, on a case-by-case basis, appropriate legal instruments or specific security protocols in order to complement this Agreement.

In witness whereof, the undersigned, duly authorised to this effect, have signed this Agreement.

Done at, on....., in two originals, each in the Lithuanian, Greek and English languages and each text being equally authentic. In case of divergence of interpretation, the English text shall prevail.

For the Government of the
Republic of Lithuania

For the Government of the
Hellenic Republic