AGREEMENT

BETWEEN

THE REPUBLIC OF LITHUANIA

AND

THE KINGDOM OF THE NETHERLANDS

CONCERNING THE EXCHANGE AND MUTUAL PROTECTION OF

CLASSIFIED INFORMATION

The Republic of Lithuania and the Kingdom of the Netherlands, hereinafter jointly referred to as "the Parties", and each individually as "Party",

in order to ensure the mutual protection of Classified Information have, in the interests of national security,

agreed upon the following:

ARTICLE 1
PURPOSE AND SCOPE

1. The purpose of this Agreement is to ensure the protection of Classified Information either exchanged between the Parties, between a Party and a Contractor under the jurisdiction of the other Party or between Contractors under the respective Parties' different jurisdictions, or generated under this Agreement. This Agreement sets out the security procedures and arrangements for such protection.

2. The Parties shall take all appropriate measures under their national laws and regulations to ensure the protection of Classified Information in accordance with this Agreement.

3. This Agreement does not constitute a basis to compel the provision or exchange of Classified Information by the Parties.

ARTICLE 2
DEFINITIONS

For the purpose of this Agreement, the following definitions mean:

a) **"Agreement"** means this document including its Annexes.

b) **"Classified Contract"** means any legally enforceable agreement to provide goods or services to be entered into by one of the Parties or a Contractor under its jurisdiction with a Contractor under the jurisdiction of the other Party, which contains Classified Information or the performance of which requires access or potential access to Classified Information. This includes pre-contractual activity.

c) **"Classified Information"** means any information, material or object, regardless of its form or nature, or any parts thereof, marked with a security classification by one of the Parties or with a security classification mutually determined by both Parties in accordance

with this Agreement, the unauthorised disclosure, alteration, compromise or loss of which could cause varying degrees of damage or harm to the interests of one or both of the Parties.

d) **"Competent Security Authority"** means the national authority, which, in accordance with laws and regulations in force in the state of the Party 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. The Competent Security Authority may delegate part of its responsibilities to a delegated competent security authority.

e) **"Contractor"** means any individual (other than those engaged by a Party under a contract of employment), legal entity or other forms of organisation (including a sub-contractor) under the jurisdiction of a Party, entering into or bound by a Classified Contract.

f) **"Facility Security Clearance"** means the positive determination by the Competent Security Authority that a facility has in place appropriate security measures to access and handle Classified Information up to and including a specified security classification level, in accordance with its national laws and regulations.

g) **"Need to Know"** means the requirement for an individual, legal entity or other form of organisation, to access, have knowledge of, or possess Classified Information in order to be able to perform their official tasks or services.

h) **"Originating Party"** means the Party under whose authority Classified Information has been created.

i) **"Personnel Security Clearance"** means the positive determination by the Competent Security Authority that an individual has been security cleared to access and handle Classified Information up to and including a specified classification level, in accordance with its national laws and regulations.

j) **"Providing Entity"** means the Party or Contractor under its jurisdiction, which provides Classified Information to the Receiving Entity under this Agreement.

k) **"Receiving Entity"** means the Party or Contractor under its jurisdiction, which receives Classified Information from the Providing Entity under this Agreement.

l) **"Security Classification Guide"** means a document associated with a Classified Contract specifying the applicable security classification levels of each part of that Classified Contract.

m) **"Security Incident"** means any unauthorised disclosure, alteration, compromise, loss, access, handling, storage or destruction of Classified Information, contrary to national laws and regulations of the Receiving Entity and/or this Agreement.

n) **"Third Party"** means any international organisation, government or state, including individuals, legal entities or other forms of organisation under its jurisdiction, which is not a Party to this Agreement.

ARTICLE 3
COMPETENT SECURITY AUTHORITIES

1. The Competent Security Authorities of the Parties are listed in the Annex of this Agreement.

2. The Competent Security Authorities shall provide each other with official contact details and changes thereof.

ARTICLE 4
SECURITY CLASSIFICATION LEVELS

The following security classifications of the Parties are equivalent and correspond to the security classification levels specified in the Parties national laws and regulations. The English equivalent is an informal translation which is not part of the national laws and regulations of the Parties and shall not be used to mark Classified Information.

The Republic of Lithuania:	**The Kingdom of the Netherlands:**	**Equivalent in English:**
VISIŠKAI SLAPTAI	Stg. ZEER GEHEIM	TOP SECRET
SLAPTAI	Stg. GEHEIM	SECRET
KONFIDENCIALIAI	Stg. CONFIDENTIEEL	CONFIDENTIAL
RIBOTO NAUDOJIMO	DEPARTEMENTAAL VERTROUWELIJK	RESTRICTED

ARTICLE 5
SECURITY MEASURES

1. The Receiving Entity shall mark all the Classified Information that it has received from the Providing Entity with the Receiving Entity's security classification that corresponds to the security classification given by the Originating Party in accordance with the scheme contained in article 4 and, where applicable, in accordance with paragraph 4 of this article. The Receiving Entity shall apply its marking to the security classification of the Providing Entity in such a way that it is always clear who is the Originating Party.

2. The Receiving Entity shall not modify or revoke the security classification of received Classified Information under this Agreement without the written approval of the Originating Party.

3. The Originating Party shall ensure that the Receiving Entity will be informed of any change in the security classification level of the Classified Information provided.

4. The Originating Party may additionally mark in English, the Classified Information with handling requirements, to specify any limitations on its use, disclosure, release and access by the Receiving Entity.

5. Classified Information jointly originated by the Parties shall be assigned a security classification that is mutually agreed upon by the Parties.

6. The Parties shall afford Classified Information exchanged or generated under this Agreement at least the same protection as they afford to their national Classified Information at the corresponding security classification level.

7. In accordance with article 1, paragraph 2 of this Agreement, the Parties shall take all appropriate measures to ensure that the Providing Entity :

a) marks Classified Information with the appropriate security classification in accordance with its national laws and regulations;

b) informs the Receiving Entity of any conditions of release or limitations on the use of the Classified Information provided.

8. In accordance with article 1, paragraph 2 of this Agreement, the Parties shall take all appropriate measures to ensure that the Receiving Entity:

a) affords the same level of protection to Classified Information as afforded to its national Classified Information of an equivalent security classification level;

b) ensures that Classified Information is not disclosed or released to a Third Party without the prior written consent of the Originating Party and if deemed necessary, on conditions;

c) uses Classified Information solely for the purpose it has been released for and in accordance with handling requirements of the Originating Party.

ARTICLE 6
ACCESS TO CLASSIFIED INFORMATION

1. Access to Classified Information shall be granted only to those individuals who have a Need to Know, are briefed on their responsibilities for the protection of Classified

Information, and have signed a statement of confidentiality in accordance with the national laws and regulations of the Receiving Entity.

2. In addition to the requirements in paragraph 1 of this article, access to Classified Information at the security classification levels equivalent to "KONFIDENCIALIAI/Stg. CONFIDENTIEEL" and above as mentioned in Article 4 of this Agreement, shall be granted only to those individuals who hold a Personnel Security Clearance at least at the corresponding level or who are otherwise duly authorized to access Classified Information by virtue of their function, in accordance with the national laws and regulations of the Receiving Entity.

ARTICLE 7
CLASSIFIED CONTRACTS

1. Upon request of the Originating Party, the Competent Security Authority of the Receiving Entity shall inform the Competent Security Authority of the Originating Party whether a Contractor, under its jurisdiction and participating in a Classified Contract or precontractual negotiations regarding a Classified Contract, has been issued a Facility Security Clearance at the required security classification level. If the Contractor does not, at that point, hold a Facility Security Clearance, or the Facility Security Clearance is at a lower level than that required, the Competent Security Authority receiving the request shall inform the requesting Competent Security Authority of that fact.

2. If a Party or a Contractor under its jurisdiction proposes to grant a Classified Contract at a security classification level equivalent to "KONFIDENCIALIAI/Stg. CONFIDENTIEEL" or above as mentioned in article 4 of this Agreement, to a Contractor under the jurisdiction of the other Party, it shall first obtain written confirmation from the Competent Security Authority of the other Party that the Contractor has been granted a Facility Security Clearance at the appropriate security classification level. For Classified Contracts at the security classification level equivalent to "RIBOTO NAUDOJIMO/DEPARTEMENTAAL VERTROUWELIJK" as mentioned in article 4 of

this Agreement, a Facility Security Clearance may be required, if stipulated by national laws and regulations of the Party under whose jurisdiction the Contractor operates.

3. In accordance with article 1, paragraph 2 of this Agreement, the Party under whose jurisdiction the Classified Contract is to be performed shall ensure that the Contractor:

a) ensures that all individuals granted access to Classified Information are informed of their responsibilities to protect Classified Information in accordance with the conditions defined in this Agreement and in accordance with their national laws and regulations;

b) monitors the security conduct within its facilities;

c) notifies promptly its Competent Security Authority of any Security Incident relating to the Classified Contract.

4. In addition to the requirements in paragraph 3 of this article, for Classified Contracts at the security classification levels equivalent to "KONFIDENCIALIAI/Stg. CONFIDENTIEEL" or above as mentioned in article 4 of this Agreement, the Competent Security Authority shall ensure that the Contractor holds a Facility Security Clearance at the corresponding security classification level in order to protect the Classified Information and that the individuals requiring access to Classified Information hold a Personnel Security Clearance at the corresponding security classification level.

5. Every Classified Contract shall include security requirements which identify the following aspects:

a) a Security Classification Guide;

b) a procedure for notification of changes in the security classification level, taking into account article 5, paragraph 3 of this Agreement;

c) the channels and procedures to be used for the transport and/or transmission of Classified Information;

d) instructions for the handling, storage, destruction and returning of Classified Information;

e) contact details of the Competent Security Authorities responsible for overseeing the protection of Classified Information related to the Classified Contract;

f) the obligation to notify any Security Incidents to the Competent Security Authority of the Contractor and the obligation for Contractors to take all reasonable steps to assist in mitigating the effect of such a security violation, in consultation with the Competent Security Authority;

g) in case a Classified Contract in whole or in part is sub-contracted to a sub-Contractor, the obligation to impose all the stipulations concerning Contractors in this Agreement to the sub-Contractor;

h) a reference to this Agreement;

i) a statement that Classified Information exchanged or generated pursuant to the Classified Contract shall be protected by the Contractor in accordance with this Agreement and applicable laws and regulations.

6. If a Classified Contract is awarded, the Party or a Contractor under its jurisdiction shall, via its Competent Security Authority, forward a copy of the security requirements to the Competent Security Authority of the Receiving Entity, to facilitate the security oversight of the Classified Contract.

7. The procedures for the approval of visits associated with Classified Contract activities by personnel of one Party to the other Party, shall be in accordance with article 8 of this Agreement.

ARTICLE 8
VISITS

1. Visits requiring access to Classified Information at a security classification level equivalent to "KONFIDENCIALIAI/Stg. CONFIDENTIEEL" or above as mentioned in article 4 of this Agreement are subject to the prior written consent of the Competent Security Authority of the host Party, unless otherwise agreed between the Competent Security Authorities. Such consent shall be given only to persons who have a Need to Know and who hold a valid Personnel Security Clearance at least at the corresponding level or who are

otherwise duly authorised to access Classified Information by virtue of their function, in accordance with the national laws and regulations of the Receiving Entity.

2. The visitor shall submit the request for visit at least ten calendar days in advance of the proposed date of the visit to his Competent Security Authority, which shall forward it to the Competent Security Authority of the other Party. In urgent cases, the Competent Security Authorities may agree on a shorter period.

3. Request for visit shall include:

a) full name of the visitor, date and place of birth, nationality and passport/ID card number;

b) official title and present position of the visitor and name of the organization the visitor represents or to which the visitor belongs;

c) confirmation of the visitor's Personnel Security Clearance and its level and validity;

d) date and duration of the visit. In the case of recurring visits the total period covered by the visits shall be stated;

e) purpose of the visit and the anticipated highest security classification level of Classified Information to be discussed or accessed;

f) name, address, phone number, e-mail address of the point of contact of the facility to be visited;

g) dated and stamped signature of a representative of the visitor's Competent Security Authority.

4. The Competent Security Authorities may agree on a list of visitors entitled to recurring visits for a period not exceeding twelve months. The Competent Security Authorities shall agree on the further details of the recurring visits.

5. The Competent Security Authority of the host Party shall inform the security officials of the facility to be visited, of the details of those individuals whose visit request has been approved. Once approval has been given, visit arrangements for individuals who have been given approval for recurring visits may be made directly with the facility concerned.

6. Classified Information provided to or acquired by a visitor shall be handled in accordance with the provisions of this Agreement.

7. The Parties shall ensure, pursuant to their national laws and regulations, the protection of the personal data of the individuals requesting for a visit requiring access to Classified Information. This personal data shall not be used for any other purpose than determining on the request for (recurring) visit.

ARTICLE 9
TRANSMISSION OF CLASSIFIED INFORMATION

1. Classified Information shall be transferred in accordance with national laws and regulations of the Originating Party or as otherwise agreed between the Competent Security Authorities.

2. Electronic transmission of Classified Information may take place only by using cryptographic means in accordance with procedures to be approved by the Competent Security Authorities.

ARTICLE 10
REPRODUCTION, TRANSLATION AND DESTRUCTION OF CLASSIFIED INFORMATION

1. Reproductions and translations of Classified Information shall be marked and placed under the same protection as the original Classified Information.

2. Reproductions and translations shall be limited to the minimum amount required for use under this Agreement.

3. Translations shall contain a suitable annotation in the language of translation, indicating that they contain Classified Information of the Originating Party.

4. Classified Information marked at the security classification level equivalent to "VISIŠKAI SLAPTAI/Stg. ZEER GEHEIM" as mentioned in article 4 of this Agreement, shall not be reproduced or translated without the prior written consent of the Originating Party.

5. Classified Information marked at the security classification level equivalent to "VISIŠKAI SLAPTAI/Stg. ZEER GEHEIM" as mentioned in article 4 of this Agreement shall be destroyed only with the prior written consent of the Originating Party. By default, it shall be returned to the Originating Party after it is no longer considered necessary by the Receiving Entity.

6. Classified Information marked up to and including the security classification level equivalent to "SLAPTAI/Stg. GEHEIM SECRET" as mentioned in article 4 of this Agreement, shall be destroyed after it is no longer considered necessary by the Receiving Entity.

7. If a crisis situation makes it impossible for a Receiving Entity to protect Classified Information provided under this Agreement, the Classified Information shall be destroyed immediately. The Receiving Entity shall, via its Competent Security Authority, notify the Competent Security Authority of the Originating Party as soon as possible and in writing of the destruction of this Classified Information.

ARTICLE 11
SECURITY CO-OPERATION

1. The Competent Security Authorities shall, on request, inform each other about changes in their national laws and regulations, policies and practices for protecting Classified Information.

2. On request of the Competent Security Authority of one Party, the Competent Security Authority of the other Party shall issue a written confirmation that a valid Personnel Security Clearance or Facility Security Clearance has been issued.

3. The Competent Security Authorities of the Parties shall recognize Personnel Security Clearances and Facility Security Clearances which are issued in accordance with the national laws and regulations of the other Party and within the scope of this Agreement.

4. The Competent Security Authorities shall assist each other in carrying out Facility Security Clearance and Personnel Security Clearance investigations on request and in accordance with their national laws and regulations.

5. The Competent Security Authorities shall promptly notify each other in writing about changes in recognised Personnel Security Clearances and Facility Security Clearances for which a confirmation has been provided.

6. The co-operation under this Agreement shall be effected in English.

ARTICLE 12
SECURITY INCIDENT

1. In case a Security Incident of the Classified Information of the Originating Party is suspected or ascertained by the Receiving Entity, it shall inform its Competent Security Authority in writing as soon as possible. The notice must contain sufficient details for the Originating Party to assess the consequences and circumstances of the suspected or actual violation.

2. The Competent Security Authorities shall immediately inform each other in writing of any actual or potential Security Incident involving Classified Information.

3. The Receiving Entity shall immediately investigate any actual or potential Security Incident. The Competent Security Authority of the Originating Party shall, if required, cooperate in the investigation.

4. The Competent Security Authority of the Receiving Entity shall take appropriate measures in accordance with its national laws and regulations to limit the consequences and to prevent a recurrence of the Security Incident. The Competent Security Authority of the Originating Party shall be informed of the outcome of the investigation and, if any, of the measures taken.

ARTICLE 13
COSTS

Each Party shall bear its own costs incurred in the course of implementing and executing its obligations under this Agreement, unless otherwise mutually determined by the Parties.

ARTICLE 14
DISPUTE RESOLUTION

Any dispute arising from the interpretation, implementation or application of this Agreement shall be settled exclusively through consultation or negotiations between the Parties and shall not be referred to any national or international tribunal or other entity for resolution.

ARTICLE 15
IMPLEMENTING ARRANGEMENTS

The Competent Security Authorities of the Parties may conclude implementing arrangements pursuant to this Agreement.

ARTICLE 16
FINAL PROVISIONS

1. This Agreement is concluded for an indefinite period of time.

2. Each Party shall notify the other Party through diplomatic channels once the national procedures necessary for entry into force of this Agreement have been completed. This Agreement shall enter into force on the first day of the second month following the receipt of the latter notification.

3. With regard to the Kingdom of the Netherlands, this Agreement shall apply to the European part of the Netherlands and the Caribbean part of the Netherlands (the islands of Bonaire, Sint Eustatius and Saba).

4. This Agreement, including its Annex, may be amended with the mutual consent of the Parties. Either Party may propose amendments to this Agreement at any time through diplomatic channels. Such amendments shall enter into force under the conditions laid down in paragraph 2 of this article, with the exception of an amendment to the Annex, which amendment shall enter into force on a date to be agreed upon by the Parties.

5. Either Party may terminate this Agreement in writing at any time through diplomatic channels. In this case, the Agreement shall expire six months after receipt of such notification.

6. In case of termination of this Agreement, all Classified Information exchanged, released or generated under this Agreement shall remain protected in accordance with the terms of this Agreement before it was terminated, for as long as the Classified Information remains classified.

IN WITNESS whereof the representatives of the Parties, duly authorised thereto, have signed this Agreement.

DONE in Vilnius on 15 July 2026 in two original copies, in the Lithuanian, Dutch and English languages, all texts being authentic. In case of divergence of interpretation, the English text shall prevail.

For the Republic of Lithuania	**For the Kingdom of the Netherlands**
	Jack Twist Quarles van Ufford

ANNEX

The Competent Security Authority for the Kingdom of the Netherlands is:
Civil National Security Authority
General Intelligence and Security Service
Ministry of the Interior and Kingdom Relations

The delegated Competent Security Authority for the Kingdom of the Netherlands in the military domain is:
Military National Security Authority
Defence Security Authority
Directorate-General of Policy
Ministry of Defence

The Competent Security Authority for the Republic of Lithuania is:
National Security Authority
The Commission for Secret Protection Coordination of the Republic of Lithuania