

AGREEMENT

BETWEEN

**THE GOVERNMENT OF
THE REPUBLIC OF BULGARIA**

AND

**THE GOVERNMENT OF
THE KINGDOM OF DENMARK**

ON

**THE MUTUAL PROTECTION
OF MILITARY CLASSIFIED
INFORMATION**

The Government of the Republic of Bulgaria and the Government of the Kingdom of Denmark (hereinafter referred to as "the Parties");

Aiming to tighten military co-operation between the Parties;

Realizing that good co-operation may require exchange or generation of Classified Information; and

Desiring to establish a set of rules regulating the mutual protection of Classified Information exchanged or generated in the course of military co-operation;

Have agreed as follows:

ARTICLE 1 OBJECTIVE AND SCOPE

1. The objective of this Agreement is to ensure the protection of Classified Information exchanged or generated in the course of military co-operation between the Parties.

2. This Agreement shall not affect the obligations of the Parties under any other bilateral or multilateral treaty, including any agreements governing exchange and mutual protection of Classified Information. If any other agreement concluded between the Parties contains stricter regulations on the exchange or protection of Classified Information, these regulations shall apply.

ARTICLE 2 DEFINITIONS

For the purpose of this Agreement:

1) **"Breach of Security"** means a deliberate or random act or an omission contrary to the national laws and regulations, the result of which may lead to actual or presumed unauthorized access to Classified Information, including, but not limited to, its disclosure, loss, destruction, damage, misappropriation or misuse.

2) **"Contractor"** means a natural or legal person or any organization or its branches possessing the legal capacity to conclude Classified Contracts in accordance with national laws and regulations.

3) **"Security Classification Level"** means a category, according to the national laws and regulations, which characterises the importance of Classified

Information, the level of restriction of access to it and the level of its protection by the Parties, and also the category on the basis of which information is marked.

4) **“Classified Contract”** means pre-contractual negotiations, a contract or a subcontract that involves or requires access to Classified Information.

5) **“Classified Information”** means any information of whatever form, nature or method of transmission generated by the ministry of defence of either Party and its subordinates or on their request, requiring under the national laws and regulations in the state of either Party protection against Breach of Security and has been duly assigned a Security Classification Level.

6) **“Competent Security Authority (CSA)”** means a Government authority which in compliance with the national legislation of the respective Party is responsible for implementing aspects of security requirements covered by this Agreement.

7) **“Facility Security Clearance”** means a positive determination following a vetting procedure to ascertain the eligibility of a legal person to have access to and handle Classified Information up to a certain Security Classification Level in accordance with national laws and regulations.

8) **“National Security Authority (NSA)”** means the Government authority of each of the Parties, which is responsible for the security of Classified Information covered by this Agreement.

9) **“Need-to-know”** means a principle by which access to Classified Information may be granted to an individual only in connection with his official duties or for his performance of a concrete official task.

10) **“Originating Party”** means the ministry of defence of either Party and its subordinates, including natural and legal persons, or their branches, which release Classified Information to the Receiving Party and are authorized to do so under the national regulations in their state.

11) **“Personnel Security Clearance”** means a positive determination following a vetting procedure to ascertain the eligibility of a person to have access to and handle Classified Information up to a certain Security Classification Level in accordance with the national laws and regulations.

12) **“Receiving Party”** means the ministry of defence of either Party and its subordinates, including natural and legal persons, or their branches, which receive Classified Information from the Originating Party and are authorized to do so under the laws and regulations in force in their state.

13) **“Third Party”** means any state including natural and legal persons or their branches under its jurisdiction or international organisations not being a party to this Agreement.

ARTICLE 3 SECURITY AUTHORITIES

1. The National Security Authorities (NSAs) designated by the Parties as responsible for the security of Classified Information covered by this Agreement are:

In the Republic of Bulgaria	In the Kingdom of Denmark
State Commission on Information Security 4 Kozloduy Str. 1202 Sofia Bulgaria	Danish Defence Intelligence Service Kastellet 30 DK-2100 Denmark

2. The NSAs shall notify each other of the relevant Competent Security Authorities (CSAs) in their countries that shall be responsible for the implementation of aspects of this Agreement.

3. The NSAs shall notify each other of any changes to their respective CSAs responsible for the implementation of this Agreement.

ARTICLE 4 CLASSIFICATION MARKINGS

1. The Parties agree that the following Security Classification Levels are equivalent and correspond to the Security Classification Levels specified in the national laws and regulations in the respective state:

For the Republic of Bulgaria	For the Kingdom of Denmark	Equivalent in the English language
СТРОГО СЕКРЕТНО	YDERST HEMMELIGT	TOP SECRET
СЕКРЕТНО	HEMMELIGT	SECRET
ПОВЕРИТЕЛНО	FORTROLIGT	CONFIDENTIAL
ЗА СЛУЖЕБНО ПОЛЗВАНЕ	TIL TJENESTEBRUG	RESTRICTED

2. The Originating Party may supplement the Security Classification Levels with further handling instructions, which detail the use of the transferred Classified Information.

3. Classified Information being created in the State of the Receiving Party on the basis of Classified Information (or part of it) transferred by the Originating Party shall be marked with the corresponding Security Classification Level which is not lower than the Security Classification Level of the transferred Classified Information.

4. The Security Classification Level of mutually generated Classified Information under this Agreement is defined by mutual consent of the Parties.

ARTICLE 5 ACCESS TO CLASSIFIED INFORMATION

Access to Classified Information under this Agreement shall be limited to individuals, who have been granted an appropriate Personnel Security Clearance, who have been informed on their responsibilities to protect Classified Information and who have "Need-to-know".

ARTICLE 6 SECURITY PRINCIPLES

1. The Receiving Party shall:

a) ensure that the received Classified Information is marked with a Security Classification Level corresponding to the Security Classification Level specified by the Originating Party in accordance with Article 4 of this Agreement;

b) afford the same degree of protection to Classified Information as afforded to its own Classified Information of an equivalent Security Classification Level;

c) ensure that Classified Information is not declassified or its protection level changed without the prior written consent of the Originating Party;

d) ensure that Classified Information is not released to a Third Party without the prior written consent of the Originating Party; and

e) use Classified Information only for the purpose for which it has been released.

2. The Originating Party shall inform the Receiving Party without undue delay of any subsequent changes to the Security Classification Level.

3. The Parties shall in due time inform each other about any changes in the national laws and regulations affecting the protection of Classified Information. In such cases, the Parties shall inform each other in written form in order to discuss possible amendments to this Agreement. Meanwhile, the Classified Information shall be protected according to the provisions of the Agreement, unless otherwise agreed in writing.

ARTICLE 7 SECURITY CO-OPERATION

1. In order to achieve and maintain comparable standards of security, each NSA shall, on request, provide the other NSA with information about the security standards, procedures and practices for protection of Classified Information, applied by the respective Party.

2. On request, the NSAs or CSAs shall, in accordance with the laws and regulations in force in their states, mutually assist in Personnel Security Clearance procedures and Facility Security Clearance procedures.

3. The Parties shall recognize the security clearances issued by the other Party in accordance with the national laws and regulations in its state. Article 4 of this Agreement shall apply correspondingly.

4. The NSAs and CSAs shall promptly notify the relevant NSA or CSA of the other Party of changes to confirmed security clearances, especially upon their revocation.

ARTICLE 8 CLASSIFIED CONTRACTS

1. Classified Contracts shall be concluded and implemented in accordance with national laws and regulations in the states of each Party. On request, the relevant NSA or CSA shall confirm that a proposed Contractor holds an appropriate Facility Security Clearance. If the proposed Contractor does not hold an appropriate Facility Security Clearance, the NSA or CSA may request that the Contractor be security cleared. Classified Contracts may only be concluded with a Contractor holding an appropriate Facility Security Clearance.

2. The NSA or CSA may request that a security inspection be carried out at a facility located in the state's territory of the other Party to ensure continued protection of Classified Information.

3. Classified Contracts shall contain a security annex on the security requirements pertaining to Classified Information. A copy of the security annex shall be forwarded to the relevant NSA or CSA.

4. The relevant NSA or CSA of the Party in whose territory the Classified Contract will 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.

5. A Contractor may appoint a subcontractor to fulfil parts of a Classified Contract. Subcontractors shall be subject to the same security requirements as those applicable to the Contractor.

ARTICLE 9

TRANSMISSION OF CLASSIFIED INFORMATION

1. Classified Information shall be transmitted between the Parties through diplomatic channels or by military couriers.

2. The Parties may transmit Classified Information electronically in accordance with security procedures approved by the relevant NSA or CSA.

3. The Receiving Party shall confirm in writing the receipt of Classified Information marked CEKPETHO/HEMMELIGT/SECRET or above. The Receiving Party shall confirm the receipt of other Classified Information upon the request of the Originating Party.

4. In connection with physical transmission of large volumes of Classified Information, the means of transmission, the route and the security measures shall be jointly determined on a case-by-case basis by the Parties' NSAs or CSAs.

5. The Originating Party shall provide Classified Information to the Receiving Party in a form which will serve the purposes of the transfer.

6. The Security and Intelligence services of the Parties may directly exchange Classified Information in accordance with the laws and regulations in force in their states.

7. Other approved means of transfer of Classified Information may only be used if agreed upon between the NSAs or CSAs.

ARTICLE 10 REPRODUCTION, TRANSLATION AND DESTRUCTION OF CLASSIFIED INFORMATION

1. Reproductions and translations of Classified Information exchanged or generated under this Agreement shall be marked with the same Security Classification Level as the original document and any additional handling instructions thereon and shall be handled with the same level of protection as the original document. The number of reproductions shall be limited to the minimum required for official purposes.

2. Any translation or reproduction of Classified Information shall be made by appropriately security cleared individuals.

3. Translations of Classified Information exchanged or generated under this Agreement shall bear a note in the language of translation indicating that they contain Classified Information provided by the Originating Party.

4. Classified Information exchanged or generated under this Agreement marked CEKPETHO/HEMMELIGT/SECRET or above shall be translated or reproduced only upon the prior written consent of the Originating Party.

5. Classified Information marked CEKPETHO/HEMMELIGT/SECRET or below may be destroyed when no longer necessary for the purposes of the transmission. For destruction of information marked CEKPETHO/HEMMELIGT/SECRET prior written consent of the Originating Party is required. The information shall be destroyed to prevent its reconstruction in whole or in part. Classified Information marked CTΠOΓO CEKPETHO/YDERST HEMMELIGT/TOP SECRET shall not be destroyed except in cases defined in paragraph 6 of this Article. It shall be returned to the Originating Party.

6. If a situation makes it impossible to protect and/or return Classified Information exchanged or created under this Agreement, the Classified Information shall be destroyed immediately. The Receiving Party shall notify the Originating Party of the destruction of the Classified Information as soon as possible.

ARTICLE 11 VISITS

1. Visits involving access to Classified Information marked **ПОБЕДИТЕЛНО /FORTROLIGT/CONFIDENTIAL** or above shall be subject to the prior written consent of the relevant NSA or CSA of the receiving party.

2. Visit requests shall be submitted at least ten days before the visit. In urgent cases, the visit request may be submitted at a shorter notice, subject to prior co-ordination between the relevant NSAs or CSAs.

3. The visitor request shall include:

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

b) official title of the visitor and specification of the legal entity represented;

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

d) date and duration of the visit; in case of recurring visits, the total period of time covered by the visits;

e) purpose of the visit, including the highest level of Classified Information to be involved; and

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

4. The NSAs or CSAs of the Parties may approve a list of authorised individuals to make recurring visits.

5. Once the lists in paragraph 4 have been approved by the NSAs or CSAs of the Parties, the terms of the concrete visits shall be directly arranged with the respective authorities of the facilities to be visited by the individuals.

6. Each Party shall protect personal data of the visitors, in accordance with its national laws and regulations.

ARTICLE 12 BREACH OF SECURITY

1. The Parties shall without undue delay mutually inform in writing of a Breach of Security.

2. The Party where the Breach of Security occurred shall investigate the incident without delay. The other Party shall, if required, co-operate in the investigation.

3. In case a breach of security occurs in a third country, the NSAs or CSAs of the dispatching Party shall take the actions under paragraph 1 and paragraph 2, where possible.

4. In any case, the other Party shall be informed of the results of the investigation and shall receive the final report on the reasons and extent of damage caused.

ARTICLE 13 EXPENSES

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

ARTICLE 14 FINAL PROVISIONS

1. This Agreement shall not apply to the Faroe Islands and Greenland. The provisions of this Agreement may be extended to the Faroe Islands and Greenland as may be agreed between the Parties in an Exchange of Notes.

2. This Agreement is concluded for an indefinite period of time. This Agreement shall enter into force on the first day of the second month following the date of receipt of the latter written notification, through diplomatic channels, stating that the national legal requirements for this Agreement to enter into force have been fulfilled.

3. This Agreement may be amended by mutual written consent of the Parties. Such amendments shall enter into force under the conditions laid down in Paragraph 2 of this Article.

4. Either Party may at any time terminate this Agreement in writing. In such a case, this Agreement shall expire six months after the receipt of the written termination notice.

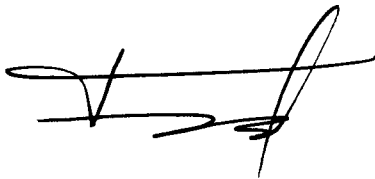
5. In case of termination of this Agreement, all Classified Information exchanged under this Agreement shall continue to be protected in accordance with the provisions of this Agreement and, upon request, returned to the Originating Party.

6. Any dispute related to the interpretation or implementation of this Agreement shall be resolved by consultations and negotiations between the Parties.

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

Done in Sofia on 21st March 2019, and in Copenhagen on 9th April 2019 in two originals, in the Bulgarian, Danish and English languages, each text being equally authentic. In case of different interpretations the English text shall prevail.

**For the Government of the Republic
of Bulgaria**



**For the Government of the Kingdom
of Denmark**

