

**AGREEMENT**

**BETWEEN**

**THE GOVERNMENT OF THE REPUBLIC OF BULGARIA**

**AND**

**THE GOVERNMENT OF THE REPUBLIC OF ARMENIA**

**ON MUTUAL PROTECTION AND EXCHANGE**

**OF**

**CLASSIFIED INFORMATION**

The Government of the Republic of Bulgaria and the Government of the Republic of Armenia (hereinafter referred to as "the Parties"),

Having agreed to negotiate on political and security issues, to expand and strengthen the cooperation between them in political, military and economic fields,

Realising the changes of the political situation in the world and acknowledging the importance of mutual cooperation for the sake of peace, international security and mutual reliability,

Acknowledging that the high level of cooperation may require exchange of Classified Information between the Parties,

Desiring to define an entity of rules on mutual protection of Classified Information, which will relate to all the agreements and contracts – comprising Classified Information – to be concluded between the States of the Parties,

Have agreed as follows:

## **Article 1**

### **Definitions**

For the purposes of this Agreement:

(1) **"Classified Information"** – information of any kind, form, mode of transmission, either created or in the process of creation, to which a Level of Classification has been attributed and which, in the interests of the national security and in accordance with the national legislation of the States of the Parties, requires protection from Unauthorised Access;

(2) **"Unauthorised Access to Classified Information"** – any form of disclosure of Classified Information, including misuse, modification, damage, disclosure, destruction or incorrect classification of Classified Information, as well as any other action compromising its protection or resulting in the loss of such information. Unauthorised Access shall be deemed to be also any action or omission resulting in knowledge of such information being acquired by any person who does not possess a Security Clearance/Security Certificate and who does not comply with the "Need-to-Know" Principle;

(3) **"Classified Document"** – any document, which includes Classified Information defined as such by the national legislation of the States of the Parties;

(4) **"Classified Material"** – any Classified Document or technical item, equipment, components or military-related products, either created or in the process of creation, as well as the components used for their creation, containing Classified Information;

(5) **“Level of Classification”** – a category, in accordance with the national legislation of the States of the Parties, which indicates the importance of Classified Information, the level of restriction of access to it and the level of its protection, as well as the category on the basis of which Classified Information is marked;

(6) **“Security Clearance/Security Certificate”** – a corresponding document issued in accordance with the national legislation of the States of the Parties as a result of a vetting procedure, which ascertains that on the matters of security a natural person/a legal entity may be granted access to Classified Information;

(7) **“Originating Party”** – the State of the Party which transmits Classified Information to the State of the other Party;

(8) **“Recipient Party”** – the State of the Party to which Classified Information is transmitted by the State of the other Party;

(9) **“Competent Authorities”** – authorities which, in accordance with the national legislation of the States of the Parties, exercise State policy in the field of protection of Classified Information in the territory of their States, are authorised to carry out general supervision in this field, as well as conduct the implementation of the provisions of this Agreement in the territory of their States. These authorities are listed in Article 5 of this Agreement;

(10) **“Contractor”** – a natural person or a legal entity which, pursuant to the provisions of this Agreement, is authorised to conclude Classified Contracts;

(11) **“Classified Contract”** – a contract, including any pre-contractual negotiations, which contains Classified Information or which involves the generation, use or transmission of Classified Information;

(12) **“Need-to-Know” Principle** – the necessity to have access to Classified Information in connection with official duties and/or for the performance of a certain official task;

(13) **“Third Party”** – a state or international organisation, which is not a Party to this Agreement;

(14) **“Declassification of Information”** – removal of the Level of Classification;

(15) **“Breach of Security”** – an act or an omission contrary to the national legislation of the States of the Parties, which results or may result in an Unauthorised Access to Classified Information.

## **Article 2**

### **Objective**

The objective of this Agreement is to ensure protection of Classified Information that is commonly generated or exchanged between the States of the Parties.

## **Article 3**

### **Levels of Classification**

The Parties have agreed that the following Levels of Classification are equivalent and correspond to the Levels of Classification set forth by the national legislation of the States of the Parties.

For the Republic of Bulgaria	For the Republic of Armenia	English equivalent
<b>СТРОГО СЕКРЕТНО</b>	<b>ՀԱՏՈՒԿ ԿԱՐԵՎՈՐՈՒԹՅԱՆ</b>	<b>TOP SECRET</b>
<b>СЕКРЕТНО</b>	<b>ՀՈՒՅԺ ԳԱՂՏՆԻ</b>	<b>SECRET</b>
<b>ПОВЕРЛИВО</b>	<b>ԳԱՂՏՆԻ</b>	<b>CONFIDENTIAL</b>

The protection of Bulgarian Classified Information at the Level of Classification **ЗА СЛУЖЕБНО ПОЛЗВАНЕ/RESTRICTED** shall be carried out in the Republic of Armenia in accordance with the **ПОВЕРЛИВО/ԳԱՂՏՆԻ/CONFIDENTIAL** Level of Classification.

## **Article 4**

### **Measures of Protection**

(1) The Parties shall, in accordance with the national legislation of their States and the requirements of this Agreement, be obliged to ensure the protection of jointly created or exchanged Classified Information.

(2) The Parties shall inform each other in due time on any changes in the national legislation of their States, which will affect the protection of Classified Information. In this case, the Parties shall inform each other in written form in order to discuss possible amendments to this Agreement. During this period, Classified Information shall be protected according to the provisions of the Agreement, unless there are other written arrangements.

(3) No individual shall be entitled to access to Classified Information solely by virtue of his or her rank, official position or Security Clearance. Access to Classified

Information shall be granted only to those individuals who have been issued a Security Clearance in accordance with the "Need-to-Know" Principle.

(4) The Recipient Party shall be obliged:

a) not to disclose and transmit Classified Information to a Third Party without relevant written consent of the Competent Authority of the Originating Party;

b) to grant Classified Information a Level of Classification equivalent to that provided by the Originating Party in accordance with Article 3;

c) not to use Classified Information for purposes other than those for which it has been transmitted.

## **Article 5**

### **Competent Authorities**

(1) The Competent Authorities of the Parties are:

- For the Republic of Bulgaria: State Commission on Information Security, Sofia, Republic of Bulgaria;

- For the Republic of Armenia: National Security Service adjunct to the Government of the Republic of Armenia, Yerevan, Republic of Armenia.

(2) The Parties notify each other through diplomatic channels of any subsequent changes of their Competent Authorities.

(3) The Competent Authorities shall inform each other on the applicable national legislation concerning the protection of Classified Information.

(4) In order to ensure closer cooperation for the purpose of implementation of this Agreement, upon request of one of the Parties, the Competent Authorities may hold consultations.

(5) In order to achieve and maintain comparable standards of security, the Competent Authorities, on request, provide each other with information about the security standards, procedures, functions and practices in the field of protection of Classified Information, applied by the respective Party.

## **Article 6**

### **Security Cooperation**

(1) In accordance with the national legislation of the Parties, State bodies authorised in the field of security, may directly exchange and return operation and/or intelligence information to each other.

(2) On request, the Competent Authorities, in accordance with their national legislation, assist mutually throughout the procedures for issuance of a Security Clearance/Security Certificate.

(3) The Parties mutually recognize their Security Clearances/Security Certificates, in accordance with their legislation.

(4) The cooperation under this Agreement is carried out in the English language.

## **Article 7**

### **Transmission of Classified Information**

(1) As a rule, Classified Information shall be transmitted through diplomatic channels.

(2) The Republic of Bulgaria may also transmit Classified Information to the Republic of Armenia through military couriers. The Republic of Armenia may also transmit Classified Information to the Republic of Bulgaria through couriers or military couriers.

(3) The Recipient Party shall immediately inform the Originating Party on the fact of receipt of Classified Information.

(4) Classified Information may be transmitted through protected communication systems, networks or other electromagnetic equipments which are approved by the Competent Authorities and possess a certificate issued in accordance with the national legislation of the States of the Parties.

(5) Other means of transmission of Classified Information may be used only upon mutual consent of the Competent Authorities.

(6) In case of transmitting large volume of Classified Information, the Competent Authorities shall grant their permission and approve the means of transmission, the route and other security measures.

**Article 8**  
**Translation, Reproduction and Destruction**  
**Changing and Removing Levels of Classification**

(1) Classified Information at the Level of Classification ЦПОГО СЕКРЕТНО/ՀԱՏՈՒԿ ԿԱՐԵՎՈՐՈՒԹՅԱՆ/TOP SECRET shall be translated and/or reproduced only upon written consent of the Originating Party.

(2) All the translations of Classified Information shall be made only by the persons who possess Security Clearance up to the appropriate Level of Classification. Such translations shall bear an equal Level of Classification in accordance with Article 3 of this Agreement.

(3) When Classified Information is reproduced, all original security markings thereon shall also be marked on each copy. Such reproduced information shall be placed under the same control as the original information. The number of copies shall be limited to that required for official purposes.

(4) Classified Information shall be destroyed in such a way as to prevent its complete or partial reconstruction.

(5) The Originating Party may prohibit the reproduction or destruction of Classified Information, giving it a special marking or attaching written notice. Where the destruction of Classified Information is prohibited, it shall be returned to the Originating Party.

(6) Classified Information at the Level of Classification ЦПОГО СЕКРЕТНО/ՀԱՏՈՒԿ ԿԱՐԵՎՈՐՈՒԹՅԱՆ/TOP SECRET shall not be subject to destruction, except for the cases envisaged by Paragraph 7 of this Article. It shall be returned to the Originating Party.

(7) In times of crises, where it is impossible to protect or return the Classified Information created and transmitted in accordance with this Agreement, it shall be destroyed immediately. The Recipient Party shall inform the Competent Authority of the Originating Party as soon as possible about the destruction of the Classified Information.

(8) All translations shall bear a designation which shows that they contain Classified Information received by the Originating Party.

(9) The Recipient Party shall not change and/or remove the Level of Classification of the received Classified Information without the prior written permission of the Originating Party.

## **Article 9**

### **Classified Contracts**

(1) A Classified Contract shall be concluded and implemented in accordance with the national legislation of the States of the Parties. Upon request, the Competent Authorities of the Parties shall provide information to each other whether a proposed Contractor has been issued a national Security Clearance/Security Certificate, corresponding to the required Level of Classification. If the proposed Contractor does not hold a Security Clearance/Security Certificate, the Competent Authority of each Party may request for that Contractor to be security cleared.

(2) A security annex shall be an integral part of each Classified Contract or subcontract. The Contractor of the Originating Party shall indicate in this annex which information should be sent to the Recipient Party or should be created by the latter. The security annex shall contain provisions on the security requirements.

(3) The obligation of the Contractor for the protection of the Classified Information shall in any case include:

a) the obligation that the Contractor shall provide Classified Information to such person who has been priorly granted Security Clearance with regard to the relevant Contract activities, who complies with the "Need-to-Know" Principle, and who is employed or is involved in the process of implementation of the Contract;

b) the means to be used for the transmission of Classified Information;

c) notification processes and mechanisms related to the changes, that may arise in respect of Classified Information either because of changes in its Level of Classification or because protection is no longer necessary;

d) the procedure for the approval of visits, access or inspection by personnel of one Party to facilities of the other Party which are covered by the Contract;

e) an obligation to notify in due time the Contractor's Competent Authority of any actual, attempted or suspected Unauthorised Access to Classified Information of the Contract;

f) usage of the Classified Information under the Contract only for the purposes related to the subject matter of the Contract;

g) strict adherence to the procedure for destruction of Classified Information;



h) an obligation that Classified Information shall be transmitted to Third Parties only upon written consent of the Competent Authority of the Originating Party.

(4) The measures required for the protection of Classified Information, as well as the procedure for assessment, reduction or compensation for the possible damage caused to Contractors, due to the Unauthorized Access to Classified Information, shall be specified in detail in the respective Classified Contract.

(5) Contracts comprising Classified Information at the Level of Classification 3A СЛУЖЕБНО ПОЛЗВАНЕ/RESTRICTED – placed by Contractors – will contain an appropriate provision which defines the minimum measures for protection of such Classified Information. Security Clearance/Security Certificate shall not be necessary for this kind of Contracts.

## **Article 10**

### **Visits**

(1) Representatives of the Competent Authorities may regularly hold consultations to discuss the procedures for protection of Classified Information.

(2) Visitors shall receive prior written authorization from the Competent Authority of the host State only if they are authorized for access to Classified Information in accordance with the legislation of their State and if they need access to facilities where Classified Information is created, processed or stored.

(3) The procedure for the visit shall be agreed between the Competent Authorities.

(4) Visits of representatives of one of the Parties to facilities of the other Party, for which access to Classified Information is required, shall be limited to those required for official purposes.

(5) The application for a visit shall contain the following information:

a) name, surname, date and place of birth of the visitor, number of the passport (other identification document);

b) nationality of the visitor;

c) position held by the visitor and name of the organisation represented thereby;

d) Security Clearance of the visitor at the appropriate Level of Classification;

e) purpose of the visit, the working programme to be presented and the planned date of visit;

f) names of the facilities to be visited.

(6) For the implementation of this Agreement recurring visits may be executed. The Competent Authorities of the Parties approve a list of authorized individuals to make recurring visits. Those lists are valid for an initial period of twelve months.

(7) Once the lists in Paragraph 6 have been approved by the Competent Authorities 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.

(8) Each Party shall, pursuant to the national legislation, guarantee the security of the personal data of the visitor.

### **Article 11**

#### **Breach of Security**

(1) In case of Breach of Security, the Competent Authority of the Party in the territory of the State of which the breach has occurred, shall immediately inform thereon in writing the Competent Authority of the other Party and conduct relevant investigation. Where appropriate, while conducting investigation the Parties may cooperate with each other.

(2) In case of Breach of Security in the territory of a Third Party, the Competent Authority of the dispatching party shall, where possible, carry out actions under Paragraph 1.

(3) The Party carrying out investigation, shall inform in writing the other Party on the results thereof, providing a final report on the reasons and extent of the damage caused.

### **Article 12**

#### **Expenses**

Each Party shall bear the expenses necessary for the exercise of its duties prescribed by this Agreement.

### **Article 13**

#### **Final Provisions**

(1) This Agreement shall be concluded for an indefinite period of time and shall enter into force on the date of receipt through diplomatic channels of the last notification on the completion by the Parties of all the internal procedures necessary for the entry into force of the Agreement.

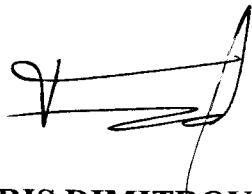
(2) Upon written consent of the Parties, amendments may be made to this Agreement. Such amendments shall enter into force in accordance with Paragraph 1 of this Article.

(3) Each Party may terminate the Agreement through a written notification addressed to the other Party. The termination shall enter into force 6 months after receipt of the notification thereon through diplomatic channels. Irrespective of the termination of this Agreement, all the Classified Information transmitted under this Agreement shall remain protected, until the Originating Party dispenses the Recipient Party from this obligation.

(4) Any dispute concerning the interpretation or application of this Agreement shall be settled through mutual understanding and consultation between the Parties, without recourse to any jurisdiction.

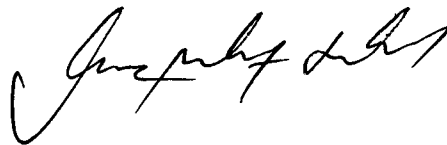
Done in Yerevan, on 12 February 2018, in two original copies, each in the Bulgarian, Armenian and English languages, all the texts being equally authentic. In case of divergences during the interpretation of the provisions of this Agreement, the English text shall prevail.

**FOR THE GOVERNMENT OF  
THE REPUBLIC OF BULGARIA**



**BORIS DIMITROV  
CHAIRPERSON OF THE  
STATE COMMISSION ON  
INFORMATION SECURITY**

**FOR THE GOVERNMENT OF  
THE REPUBLIC OF ARMENIA**



**EDWARD NALBANDIAN  
MINISTER OF FOREIGN AFFAIRS**