

**AGREEMENT**

**BETWEEN**

**THE GOVERNMENT OF THE REPUBLIC**

**OF BULGARIA**

**AND**

**THE GOVERNMENT OF THE REPUBLIC**

**OF MACEDONIA**

**ON EXCHANGE AND MUTUAL PROTECTION**

**OF THE CLASSIFIED INFORMATION**

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

Having agreed to hold talks on political and security-related issues and to broaden and tighten the political, military and economic co-operation,

Being aware of the changes in the political and military situation in the world and recognising the important role of their mutual co-operation for the stabilisation of peace, international security and mutual confidence,

Realising that good co-operation may require exchange of Classified Information between the Contracting Parties,

Desiring to create a set of rules regulating the mutual protection of Classified Information applicable to any future co-operation agreements and Classified contracts, which will be implemented between the Contracting Parties, containing or involving Classified Information,

Have agreed as follows:

### **Article 1** **Definitions**

For the purpose of this Agreement:

(1) "**Classified Information**" means:

- for the Republic of Bulgaria: information, determined in accordance with the national laws and regulations, the Unauthorized access to which could cause danger for or could damage the interests of the Republic of Bulgaria related to the national security, defence, foreign policy or protection of constitutionally established order;
- for the Republic of Macedonia: information which is protected by unauthorized access or use and which is determined with Security classification level.

(2) **"Unauthorised access"** means any form of disclosure, misuse, change, damage, submission, destruction of Classified Information, as well as any other actions, resulting in breach of protection or loss of such information. For Unauthorized access is considered also any omission to classify information with appropriate Security classification level or incorrect classification as well as any action or inaction that have resulted in making the information known by a person who does not possess an appropriate clearance or confirmation.

(3) **"Classified document"** means any recorded Classified Information, regardless of its physical form or characteristics, including the following carriers of information: handwritten or typed paper, seals, programmes used for processing data, maps, tables, photographs, pictures, pigmentation, engravings, drawings or parts thereof, sketches, rough copies, notes, ink ribbons, carbon copies or for reproducing by any means or process sounds, voices, magnetic or video or electronic or optical recordings in any form, as well as portable Automatic Data Processing equipment with a fixed or removable data storage carrier, etc.

(4) **"Classified material"** means any document or technical item, equipment, installation, device or weapon either manufactured or in process of manufacture, as well as components used for their manufacture, containing Classified Information.

(5) **"Security classification level"** means category which according to the national laws and regulations characterises the importance of the Classified Information, the level of restriction of access to it and the level of its protection by the Contracting Parties and also category on the basis of which the appropriate information is marked.

(6) **"Classification marking"** means a mark on any Classified material which shows the Security classification level.

(7) **"Personnel Security Clearance/Facility Security Clearance"** means a positive determination stemming from a vetting procedure that shall ascertain loyalty and trustworthiness of an individual or legal entity as well as other security aspects in accordance with national laws and regulations. Such determination enables to grant the individual or the legal entity access and allow them to handle Classified Information on a certain level without security risk.

- (8) **"Originating Party"** means the party initiating Classified Information.
- (9) **"Receiving Party"** means the party to which Classified Information is transmitted.
- (10) **"Competent authority"** means the authority, which in accordance with the national laws and regulations of the respective Contracting Party performs the state policy for the protection of Classified Information, exercises overall control in this sphere as well as conducts the implementation of this Agreement. Such authorities are listed in Article 5 of this Agreement.
- (11) **"User"** means a legal entity or an individual which takes part in relevant co-operation activities or in implementation of Classified contracts to which this Agreement will be applied.
- (12) **"Classified contract"** means an agreement between two or more users which contains or provides for access to Classified Information.
- (13) **"Contractor"** means an individual or a legal entity possessing the legal capacity to conclude contracts and/or a party to a Classified contract under the provisions of this Agreement.
- (14) **"Third party"** means any subject who does not respond to the need-to-know principle and who is not granted access.
- (15) **"Declassification of Information"** means removal of the Security classification level.

## **Article 2**

### **Objective**

Objective of this Agreement is the protection of Classified Information, exchanged either directly or indirectly between the Contracting Parties.

## **Article 3**

### **Security classification levels**

The Contracting Parties agree that the following Security classification levels are equivalent and correspond to the Security classification levels

determined in the national laws and regulations of the respective Contracting Party:

For the Republic of Bulgaria	Equivalent in English	For the Republic of Macedonia
СТРОГО СЕКРЕТНО	TOP SECRET	ДРЖАВНА ТАЈНА
СЕКРЕТНО	SECRET	СТРОГО ДОВЕРЛИВО
ПОВЕРИТЕЛНО	CONFIDENTIAL	ДОВЕРЛИВО
ЗА СЛУЖЕБНО ПОЛЗВАНЕ	RESTRICTED	ИНТЕРНО

#### **Article 4**

##### **Measures for Classified Information protection at national level**

(1) In compliance with their national laws and regulations, the Contracting Parties shall implement all appropriate measures for protection of Classified Information, which shall be submitted under this Agreement or generated under a Classified contract. The same level of protection shall be ensured for such Classified Information as it is provided for the national Classified Information with the corresponding Security classification level.

(2) The Contracting Parties shall in due time inform each other about any changes in the national laws and regulations affecting to the protection of Classified Information. In such cases, the Contracting Parties shall inform each other in compliance with Paragraphs 3 and 4 of Article 5 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.

(3) No individual shall be granted access to Classified Information solely by virtue of his/her rank, official position or Personnel Security Clearance/Facility Security Clearance. Access to Classified Information shall be granted only to those individuals who have been issued Personnel Security Clearance/Facility Security Clearance in accordance with the national laws and regulations of the Contracting Party and if their official position requires such access.

(4) The Receiving Party is obligated:

- a) not to submit Classified Information to a Third party without prior written consent of the Originating party;
- b) to grant Classified Information Security classification level equivalent to that provided by the Originating party;
- c) not to use the Classified Information for other purpose other than that it has been provided for;
- d) to guarantee the private rights such as patent rights, copyrights or trade secrets that are involved in the Classified Information.

(5) If any other agreements concluded between the Contracting Parties contain stricter regulations regarding the exchange or protection of the Classified Information, these regulations shall apply.

## **Article 5**

### **Competent authorities**

(1) The Competent authorities of the Contracting Parties are:

For the Republic of Bulgaria:

- State Commission on Information Security;

For the Republic of Macedonia:

- Directorate for Security of Classified Information.

(2) The Competent authorities shall provide each other with their official requisites.

(3) The Competent authorities shall inform each other of the national laws and regulations in force regulating the protection of Classified Information.

(4) In order to ensure closer co-operation in the implementation of this Agreement, the Competent authorities may hold consultations at the request made by one of them.

(5) In order to achieve and maintain comparable standards of security, the Competent authorities shall, on request, provide each other with information about the security standards, procedures and practices for protection of Classified Information in the respective Contracting Party.

(6) The Competent authorities may conclude executive documents in relation with this Agreement.

## **Article 6**

### **Transfer of Classified Information**

(1) As a rule, Classified Information shall be transferred by means of diplomatic or military couriers. The Receiving party shall confirm in writing the receipt of Classified Information.

(2) Classified Information may be transmitted via protected telecommunication systems, networks or other electromagnetic means approved by the competent authorities and holding a duly issued certificate pursuant to the national laws and regulations of the Contracting Parties.

(3) Other approved means of transfer of Classified Information may only be used if agreed upon between the Competent authorities.

(4) In case of transferring a large consignment containing Classified Information, the Competent authorities shall mutually agree on and approve the means of transportation, the route and the other security measures.

## **Article 7**

### **Translation, reproduction, destruction**

(1) The Classified materials containing information with a Security classification level **CTPOFO CEKPETHO/ TOP SECRET/ ДРЖАБНА TAJHA** shall be translated or reproduced only by written permission of the Competent authority of the Originating party.

(2) All translations of Classified Information shall be made by individuals who possess issued appropriate Personnel Security Clearances. Such translations shall bear an appropriate Classification marking and a suitable annotation in the language of the translation, indicating that the translation is containing Classified Information of the Originating party.

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

(4) Classified materials shall be destroyed or modified insofar as to prevent their reconstruction in whole or in part.

(5) The Originating party may expressly prohibit reproduction, alteration or destruction of a Classified material or document by marking the relevant carrier of Classified Information or sending subsequent written notice. In such case the Classified material or document needed to be destroyed shall be returned to the Originating party.

## **Article 8**

### **Classified contracts**

(1) Classified contracts shall be concluded and implemented in accordance with the national laws and regulations of each Contracting Party. Upon request the Competent authority of each Contracting Party shall furnish information whether a proposed Contractor has been issued a national Personnel Security Clearance / Facility Security Clearance, corresponding to the required Security classification level. If the proposed Contractor does not hold a Personnel Security Clearance / Facility Security Clearance the Competent authority of each Contracting Party may request for that Contractor to be security cleared for issuance of a Personnel Security Clearance / Facility Security Clearance.

(2) A security annex will be an integral part of each Classified contract or sub-contract. In this annex the Contractor of the Originating party will specify which Classified Information will be released to or generated by the Receiving party, and which corresponding Security classification level has been assigned to this information.

(3) The Contractor's obligation to protect the Classified Information shall, in all cases, refer, at least, to the following:

- a) an obligation for the Contractor to disclose Classified Information only to a person who has been previously security cleared for access with regard to the relevant contract activities, who has need-to-know and who is employed or engaged in the performing of the contract;
- b) to refuse access to Classified Information to any person who has not received a Personnel Security Clearance in connection to the respective contract activities, who has no need-to-know and is not employed or engaged in the performing of the contract;
- c) the channels to be used for the transfer of Classified Information;



- d) the procedures and mechanisms for communicating the changes that may arise in respect of Classified Information either because of changes in its Security classification level or because its protection is no longer required;
- e) the procedure for the approval of visits, access or inspections by personnel of one of the Contracting Parties to the facilities of the other Contracting Party which are connected to the contract;
- f) an obligation the Contractor's Competent authority to be notified of any actual, attempted or suspected Unauthorised access to Classified Information, related to the contract;
- g) usage of Classified Information under the contract only for the purposes related to the subject of the contract;
- h) strict adherence to the procedures for destruction of Classified Information and materials;
- i) releasing of Classified Information under the contract to any Third party only with the explicit consent of the Competent authority of the Originating party.

(4) The measures required for protection of the Classified Information as well as the procedure for assessment of and indemnification for possible losses caused to the Contractors by Unauthorised access to Classified Information shall be specified in more details in the respective Classified contract.

(5) Contracts concluded with Contractors involving Classified Information at 3A СЛЮЖЕБНО ПОЛЗБАНЕ/ RESTRICTED/ ИНТЕРНО Security classification levels will contain an appropriate clause identifying the minimum measures to be applied for the protection of such Classified Information. It is not needed for the Contractors to possess a Personnel Security Clearance/Facility Security Clearance in order to obtain information with Security classification level 3A СЛЮЖЕБНО ПОЛЗБАНЕ/ RESTRICTED/ ИНТЕРНО.

## **Article 9**

### **Visits**

(1) Security experts of the Competent authorities may hold regular meetings to discuss the procedures for protection of the Classified Information.

(2) When access to Classified Information or to premises where Classified Information is originated, handled or stored is needed, the visitors shall receive prior authorization from the Competent authority of the host state.

(3) The visiting procedures shall be agreed between the Competent authorities.

(4) Each Contracting Party shall guarantee the protection of the personal data of the visitors on its own territory, according to the respective national laws and regulations.

### **Article 10**

#### **Breach of Security**

(1) In case of a breach of security, which has led to real or possible Unauthorised access or disclosure of Classified Information, created or received by the other Contracting Party, the Competent authority of the Contracting Party, where a breach of security has occurred, shall inform the Competent authority of the other Contracting Party as soon as possible and shall carry out the appropriate investigation. The other Contracting Party shall, if required, cooperate in the investigation.

(2) In cases when the Unauthorised access or disclosure has occurred in a state other than the Contracting Parties, the Competent authority of the sending Contracting Party shall take the actions described in paragraph 1.

(3) In any case, the other Contracting Party shall be informed of the results of the investigation and shall receive the final report on the reasons and extent of the damages.

### **Article 11**

#### **Expenses**

Each Contracting Party shall bear the expenses related to implementation of its obligations under this Agreement.

### **Article 12**

#### **Final Provisions**

(1) This Agreement is concluded for an indefinite period of time and enters into force on the date of receiving the latest notice whereby the Contracting

Parties inform each other by diplomatic channels of the fulfilment of all internal legal procedures necessary for its entry into force.

(2) On mutual consent of the Contracting Parties this Agreement may be amended in written form and such amendments shall enter into force in accordance with the procedures for entering into force of this Agreement.

(3) Each Contracting Party may terminate this Agreement by written notification sent through the diplomatic channels. The termination shall enter into force 6 (six) months after the date of receipt of the notification for the termination by the other Contracting Party. Notwithstanding the termination of this Agreement, all Classified Information transferred pursuant to this Agreement shall continue to be protected in accordance with the provisions set forth herein, until the Originating party dispenses the Receiving party from this obligation.

(4) Any dispute regarding the interpretation or application of this Agreement shall be resolved amicably by consultations and negotiations between the Contracting Parties without recourse to outside jurisdiction.

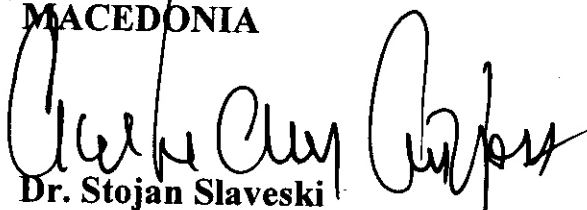
Done on 7 October 2005 year, in Blagoevgrad in 2 original copies, each in the Bulgarian language in accordance with the Constitution of the Republic of Bulgaria, Macedonian language in accordance with the Constitution of the Republic of Macedonia and English language, all texts being equally authentic. In case of any divergence of interpretation, the English language text shall prevail.

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



**Tsveta Markova  
Chairperson of the State  
Commission on Information  
Security**

**FOR THE GOVERNMENT  
OF THE REPUBLIC OF  
MACEDONIA**



**Dr. Stojan Slaveski  
Director of the Directorate for  
Security of Classified  
Information**