

**AGREEMENT**

**BETWEEN**

**THE GOVERNMENT OF THE REPUBLIC OF  
BULGARIA**

**AND**

**THE GOVERNMENT OF THE REPUBLIC OF  
SLOVENIA**

**ON**

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

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

realising that mutual co-operation may require exchange of Classified Information between the Parties,

wishing to ensure the protection of Classified Information exchanged between the Parties or between public and private entities under their jurisdiction,

have agreed as follows:

## **ARTICLE 1**

### **DEFINITIONS**

For the purposes of this Agreement these terms mean the following:

- a) **"Classified Information"**: Any information, document or material, regardless of its form, transmitted or generated between the Parties, which requires protection against unauthorized access and is designated as such and marked appropriately in accordance with the national laws and regulations of either Party.
- b) **"Originating Party"**: The Party, including any public or private entities under its jurisdiction, which releases Classified Information to the Recipient Party.
- c) **"Recipient Party"**: The Party, including any public or private entities under its jurisdiction, which receives Classified Information from the Originating Party.
- d) **"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.
- e) **"Personnel Security Clearance"**: A positive determination following an accomplished vetting procedure in accordance with

national laws and regulations, on the basis of which an individual is eligible to have access to and to handle Classified Information up to the level defined in the clearance.

- f) **“Facility Security Clearance”**: A positive determination following an accomplished vetting procedure that a Contractor has the capability to handle Classified Information, in accordance with national laws and regulations.
- g) **“Contractor”**: An individual or a legal entity possessing the capacity to contract.
- h) **“Classified Contract”**: A contract or a sub-contract, including pre-contractual negotiations, which contains Classified Information or involves access to it.
- i) **“Third Party”**: A state, including any public or private entities under its jurisdiction, or an international organisation that is not a Party to this Agreement.
- j) **“Unauthorised access”**: Any form of disclosure of Classified Information, including misuse, damage, submission and incorrect classification thereof, as well as any other actions, resulting in breach of protection or loss of such information, as well as any actions or omissions that have resulted in making the information known to an unauthorised person.
- k) **“Security classification level”**: The category which under the national laws and regulations characterises importance of Classified Information, level of restriction of access to it and of its protection by the Parties.
- l) **“National Security Authority”**: The authority, which in compliance with the national laws and regulations is responsible for the general implementation and the relevant controls of all aspects of this Agreement.
- m) **“Breach of security”**: An action or an omission contrary to the national laws and regulations, which results or may result in an unauthorised access or destruction of Classified Information.

## **ARTICLE 2**

### **OBJECTIVE**

In accordance with their national laws and regulations and in respect of national interests and security both Parties shall take all appropriate measures to ensure the protection of Classified Information, which is transmitted or generated according to this Agreement.

## **ARTICLE 3**

### **NATIONAL SECURITY AUTHORITIES**

(1) The National Security Authorities of The Parties are:

- In the Republic of Bulgaria:

State Commission on Information Security;

- In the Republic of Slovenia:

Government Office for the Protection of Classified Information.

(2) The Parties shall inform each other through diplomatic channels of any subsequent changes of the National Security Authorities.

## **ARTICLE 4**

### **SECURITY CLASSIFICATION LEVELS**

(1) Classified Information released under this Agreement shall be marked with the appropriate Security classification level in accordance with the national laws and regulations of the Parties.

(2) The following national Security classification levels are equivalent and correspond to the Security classification levels specified in the national laws and regulations of the Parties:

<b>Republic of Bulgaria</b>	<b>Republic of Slovenia</b>	<b>English translation</b>
СТРОГО СЕКРЕТНО	STROGO TAJNO	TOP SECRET
СЕКРЕТНО	TAJNO	SECRET
ПОВЕРИТЕЛНО	ZAUPNO	CONFIDENTIAL
ЗА СЛУЖЕБНО ПОЛЗВАНЕ	INTERNO	RESTRICTED

## **ARTICLE 5**

### **PROTECTION OF CLASSIFIED INFORMATION**

- (1) The Parties shall afford to Classified Information referred to in this Agreement the same protection as to their own Classified Information of the corresponding Security classification level.
- (2) Access to Classified Information shall be allowed only to those individuals with a Need-to- Know, who have been briefed on handling and protection of Classified Information and who have been duly authorised in accordance with national laws and regulations.
- (3) The Parties shall mutually recognise their Personnel Security Clearances and Facility Security Clearances. Article 4 shall apply accordingly.
- (4) The Originating Party shall:
  - a) ensure that the 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 the Classified Information and of any subsequent changes in the Security classification levels and/or the eventual declassification.
- (5) The Recipient Party shall:
  - a) ensure that the Classified Information is marked with an equivalent security classification level in accordance with Paragraph 2 of Article 4, and

- b) ensure that the Security classification level is not changed unless authorized in writing by the Originating Party.
- (6) The Parties shall in due time inform each other about changes in the national laws and regulations affecting the protection of Classified Information.
- (7) Each Party shall ensure that appropriate measures are implemented for the protection of Classified Information 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 6**

### **RESTRICTION OF USE OF CLASSIFIED INFORMATION**

- (1) The Recipient Party shall use Classified Information only for the purpose for which it has been released and within the limitations stated by the Originating Party.
- (2) The Recipient Party shall not release Classified Information to a Third Party without a prior written consent of the Originating Party.

## **ARTICLE 7**

### **TRANSMISSION OF CLASSIFIED INFORMATION**

- (1) Classified Information shall be transmitted by diplomatic, military or other channels in accordance with the national laws and regulations of the Parties.
- (2) Other approved channels of transmission of Classified Information may only be used if agreed upon between the National Security Authorities.
- (3) In case of transferring a large consignment containing Classified Information, the National Security Authorities shall mutually agree on and approve the means of transportation, the route and the other security measures.

## ARTICLE 8

### REPRODUCTION, TRANSLATION AND DESTRUCTION OF CLASSIFIED INFORMATION

- (1) All reproductions and translations shall be marked with the appropriate Security classification levels and they shall be protected as the original Classified Information. The translations and the number of reproductions shall be limited to the minimum required for an official purpose.
- (2) All translations shall be marked with the original Security classification level and shall contain a suitable annotation, in the language of translation, indicating that they contain Classified Information of the Originating Party.
- (3) Classified Information marked **CTΠOΓO CEKPETHO/STROGO TAJNO/TOP SECRET**, both original and translation, shall be reproduced only upon the written permission of the Originating Party.
- (4) Classified Information marked **CTΠOΓO CEKPETHO/STROGO TAJNO/TOP SECRET** shall not be destroyed. It shall be returned to the Originating Party after it is no longer considered necessary by the Parties.
- (5) Information classified as **CEKPETHO/TAJNO/SECRET** or below shall be destroyed after it is no longer considered necessary by the Recipient Party, in accordance with the national laws and regulations.
- (6) In situation in which it is impossible to protect or return Classified Information transmitted or generated under this Agreement, the Classified Information shall be destroyed immediately. The Recipient Party shall inform the National Security Authority of the Originating Party about this destruction as soon as possible.
- (7) Classified Information shall be destroyed or modified in such a manner as to eliminate the possibility of its partial or total reconstruction.
- (8) If destruction of the Classified Information is prohibited, it shall be returned to the Originating Party.

## **ARTICLE 9**

### **CLASSIFIED CONTRACTS**

- (1) Classified Contract shall be concluded and implemented in accordance with national laws and regulations of each Party. Upon request the National Security Authority of each Party shall furnish information whether a contractor, sub-contractor and potential contractor has been issued an appropriate Facility Security Clearance and Personnel Security Clearance to perform functions which require access to the Classified Information.
- (2) Before providing Classified Information related to a Classified Contract to contractors, sub-contractors or potential contractors, the National Security Authority of the Recipient Party shall ensure that such contractor, sub-contractor or potential contractor fulfils the conditions to protect the Classified Information in accordance with the national laws and regulations.
- (3) Each National Security Authority may request that a security inspection is carried out at the contractor or sub-contractor involved in Classified Contract to ensure continuing compliance with security standards in accordance with the national laws and regulations.
- (4) A Classified Contract shall contain a security annex with provisions on the security requirements and on the classification of each aspect or element of the Classified Contract. A copy of such document shall be submitted to the National Security Authorities of the Parties.
- (5) Contracts placed with contractors involving Classified Information at 3A СЛЮЖЕБНО ПОЛЗБАНЕ/INTERNO/RESTRICTED levels will contain an appropriate clause identifying the minimum measures to be applied for the protection of such Classified Information.

## **ARTICLE 10**

### **VISITS**

- (1) Visits necessitating access to Classified Information shall be subject to prior permission of the National Security Authority of the host Party.

(2) A request for visit shall be submitted to the relevant National Security Authority at least 20 days prior to the commencement of the visit. The request for the visit shall include the following data that shall be used for the purpose of the visit only:

- a) the visitor's name, date and place of birth, citizenship and identification card/passport number;
- b) the visitor's position, with a specification of the employer which the visitor represents;
- c) a specification of the project in which the visitor participates;
- d) the validity and level of the visitor's Personnel Security Clearance, if required;
- e) the name, address, phone/fax number, e-mail and point of contact of the entity 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. In case of recurring visits the total period covered by the visits shall be stated;
- h) the date and signature of the sending National Security Authority.

(3) In urgent cases, the National Security Authorities can agree on a shorter period for the submission of the request for visit.

(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 12 months and may be extended for a further period of time not exceeding 12 months. A request for recurring visits shall be submitted in accordance with Paragraph 2 of this Article. Once the list has been approved, visits may be arranged directly between the subjects involved.

(5) Each Party shall guarantee the protection of personal data of the visitors in accordance with the national laws and regulations.

- (6) Any Classified Information acquired by a visitor shall be considered as Classified Information under this Agreement.

## **ARTICLE 11**

### **SECURITY CO-OPERATION**

- (1) In order to achieve and maintain relevant 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. To this aim the National Security Authorities may visit each other.
- (2) The National Security Authorities shall inform each other of exceptional security risks that may endanger the released Classified Information.
- (3) On request, the National Security Authorities shall assist each other in carrying out security clearance procedures.
- (4) The National Security Authorities shall promptly inform each other about any changes in mutually recognized Personnel Security Clearances and Facility Security Clearances.
- (5) In order to ensure close co-operation in the implementation of the present Agreement, the National Security Authorities may hold consultations at the request made by one of them.
- (6) Implementing arrangements may be concluded between the National Security Authorities for the implementation of this Agreement.

## **ARTICLE 12**

### **BREACH OF SECURITY**

- (1) In case of a breach of security, the National Security Authority in whose state a breach of security occurred shall inform the National Security Authority of the other Party as soon as possible and shall carry out the appropriate investigation. On request, the appropriate authority of the Originating Party shall cooperate in the investigation.

- (2) In case a breach of security occurs at a Third Party, the National Security Authority of the dispatching Party shall take the actions under paragraph 1 of this Article, where possible.
- (3) 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 implementation of this Agreement.

### **ARTICLE 14**

#### **SETTLEMENT OF DISPUTES**

Any dispute regarding the interpretation or application of this Agreement shall be settled by consultations and negotiations between the Parties and shall not be referred to any international tribunal or Third Party for settlement.

### **ARTICLE 15**

#### **FINAL PROVISIONS**

- (1) This Agreement shall enter into force on the first day of the second month from the date of receipt of the latest written notification by which the Parties have informed each other, through diplomatic channels, that their internal legal requirements necessary for its entry into force have been fulfilled.
- (2) This Agreement may be amended by mutual written consent of the Parties. Amendments shall enter into force in accordance with paragraph 1 of this Article.

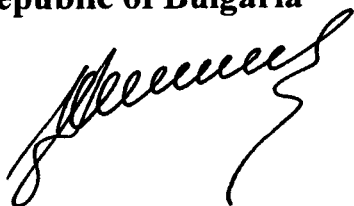
(3) This Agreement is concluded for an indefinite period of time. Either Party may denounce this Agreement by giving the other Party notice in writing through diplomatic channels. In that case, this Agreement shall terminate six months from the date on which the other Party has received the denunciation notice.

(4) In case of 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 and, upon request, returned to the Originating Party.

In witness whereof the undersigned, being duly authorised thereto, have signed this Agreement.

Done in *Predoslie* ..... on *9 May 2012* ..... in two originals in the Bulgarian, Slovenian and English languages, all texts being equally authentic. In case of any divergence of interpretation, the English text shall prevail.

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



**For the Government of the  
Republic of Slovenia**

