

**AGREEMENT**  
**Between the Government of the Republic of Bulgaria and the Government**  
**of the Republic of Cyprus on the Mutual Protection of Classified**  
**Information**

The Government of the Republic of Bulgaria and the Government of the Republic of Cyprus hereinafter referred to as "Parties".

Having due regard for guaranteeing the mutual protection of all information which has been classified pursuant to the internal laws of either Party and transmitted to the other Party.

Being guided by creation of regulation in the scope of the mutual protection of Classified Information, which is to be binding in relation to all mutual cooperation connected with the exchange of Classified Information.

Have agreed as follows:

**Article 1**  
**Definitions**

For the purpose of this Agreement:

- (1) "**Competent Authorities**" – means legal entities authorised to transmit, receive, store, protect and use Classified Information in accordance with the internal laws of their Party.
- (2) "**Competent Security Authorities**" - means state authorities, which are competent for the protection of Classified Information, as these authorities are referred to in Article 4, Paragraph 1 of this Agreement.
- (3) "**Contractor**" - means an individual or a legal entity which has legal capacity to conclude contracts.
- (4) "**Classified Contract**" - means an agreement regulating enforceable rights and obligations between the contractors, the performance of which involves access to Classified Information or originating of such information.

(5) "**Classified Information**" means information of whatever form, nature or method of transmission either manufactured or in the process of manufacture to which a security classification level has been attributed and which, in the interests of national security and in accordance with the internal laws, require protection against unauthorised access or destruction.

(6) "**Principal/Contracting authority**" means a legal entity, which intends to conclude or concludes a Classified Contract in the territory of the State of the other Party.

(7) "**Need-to-know principle**" means the necessity to have access to Classified Information in connection with official duties and/or for the performance of a concrete official task.

(8) "**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 the internal laws. 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.

(9) "**Third Party**" means a state or international organisation, which is not a Party to this Agreement.

(10) "**Unauthorised access to Classified Information**" means any form of disclosure of Classified Information, including misuse, damage, submission, as well as any other actions, resulting in breach of protection or loss of such information, as well as any actions or inactions that have resulted in making the information known to an unauthorised person.

## **Article 2**

### **Objective**

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



### Article 3

#### The Categorization of Classified Information

(1) Classified Information is granted a security classification level in accordance to its content, pursuant to the internal laws of each Party. Received Classified Information shall be granted equivalent security classification level, according to the provisions of Paragraph 4.

(2) The obligation referred to in Paragraph 1 shall also apply to Classified Information generated as a result of mutual co - operation between the Parties or the Competent Authorities, including this originated in connection with the performance of the Classified Contract.

(3) The security classification level shall be changed or removed only by the Competent Authority, which has granted it. The recipient shall be immediately notified on every change or removal of security classification level.

(4) The Parties agree that the following security classification levels are equivalent:

Republic of Bulgaria	Republic of Cyprus	English Equivalent
СТРОГО СЕКРЕТНО	ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ	TOP SECRET
СЕКРЕТНО	ΑΠΟΡΡΗΤΟ	SECRET
ПОВЕРИТЕЛНО	ΕΜΠΙΣΤΕΥΤΙΚΟ	CONFIDENTIAL
ЗА СЛУЖЕБНО ПОЛЗВАНЕ	ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ	RESTRICTED

### Article 4

#### Competent Security Authorities

(1) For the purpose of this Agreement, the Competent Security Authorities shall be:

- a. For the Republic of Bulgaria:
  - State Commission on Information Security
- b. For the Republic of Cyprus:
  - The National Security Authority

(2) The Competent Security Authorities may conclude implementation agreements or/and executive documents for the purpose of the implementation of the provisions hereof.

## **Article 5**

### **Principles of Classified Information Protection and National measures**

- (1) In accordance with this Agreement and their internal laws, the Parties shall adopt appropriate measures aimed at the protection of Classified Information which is transmitted or originated as a result of mutual co-operation between both Parties or the Competent Authorities, including this originated in connection with the performance of a Classified Contract.
- (2) The Parties shall provide for the information referred to in Paragraph 1 at least the same protection as applicable to their own Classified Information under the relevant security classification level, pursuant to Article 3, Paragraph 4.
- (3) Received Classified Information shall be used exclusively for the purposes defined at the transmission thereof.
- (4) Either Party shall not release the information referred to in Paragraph 1 to any third parties without a prior written consent of the Competent Authority of the other Party, which granted adequate security classification level.
- (5) The Competent Security Authorities shall ensure necessary control over Classified Information protection.
- (6) Received Classified Information shall be accessible only to those persons who have a need-to-know, who have been security cleared and who have been authorized to have access to such information as well as briefed in the scope of Classified Information protection according to the internal laws of their Party.
- (7) The Parties shall in due time inform each other about any changes in the internal laws, affecting the protection of Classified Information.

## **Article 6**

### **Classified Contracts**

- (1) The Principal / Contracting Authority may conclude a Classified Contract with the Contractor located in the territory of one of the Parties.
- (2) Classified Contract shall be concluded and implemented in accordance with



internal laws of each Party. Upon request the Competent Security Authority of each Party shall provide written assurance whether a proposed contractor has been issued a national security clearance, corresponding to the required security classification level. In the case when the Proposed contractor does not hold a security clearance, the Competent Authority of each Party may request for that contractor to be security cleared.

(3) The issuing of the assurance referred to in Paragraph 2 shall be the amount to a guarantee that the Contractor fulfils the criteria in the scope of the protection of Classified Information, as specified in the internal laws of the Party in whose territory the Contractor is located.

(4) Classified Information shall not be accessible to the Contractor until the receipt of the assurance referred to in Paragraphs 2 and 3.

(5) A security annex will be an integral part of each Classified Contract or sub-contract. In this annex the Principal/Contracting Authority shall specify which Classified Information will be released to or generated by the Contractor and which corresponding security classification level has been assigned to this information.

(6) The Competent Security Authority of the Party in whose territory the Classified Contract is to be performed shall ensure that the Contractor protects Classified Information transmitted by the Principal / Contracting Authority or originated during the performance of the Classified Contract in accordance with the Security annex, as referred to in Paragraph 5 and the internal laws of its Party.

(7) The performance of the Classified Contract in the part connected with access to Classified Information shall be allowed upon the Contractor's meeting the criteria necessary for the protection of Classified Information, according to the Security annex, as referred to in Paragraph 5.

(8) The Competent Security Authorities shall ensure that any possible subcontractors shall comply with the same conditions for the protection of Classified Information as those laid down for the Contractor.

(9) For Classified Contracts involving 3A СЛУЖЕБНО ПОЛІЗБАНЕ/ ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ/ RESTRICTED Classified Information security clearance is not issued.

## **Article 7**

### **Transmission of Classified Information**

(1) Classified Information shall be transmitted through diplomatic channels or through other channels ensuring its protection against unauthorized disclosure, agreed upon between the Competent Security Authorities of both Parties. 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, which have been accredited for use pursuant to the internal laws of either of the Parties.

## **Article 8**

### **Reproduction and Translation of Classified Information**

(1) Information classified as ΤΡΟΓΟ ΣΕΚΡΕΤΗΟ/ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ/TOP SECRET shall be reproduced only after a prior written permission issued by the Competent Authority, which provided this information.

(2) Reproduction of Classified Information shall be pursuant to the internal laws of each of the Parties. Reproduced information shall be placed under the same protection as the originals. Number of copies shall be reduced to that required for official purposes. The Originator may expressly prohibit reproduction of a Classified Information by marking the relevant carrier or sending subsequent written notice.

(3) Any translation of Classified Information shall be made by properly security cleared individuals. All translations shall bear an appropriate note in the language into which they have been translated, stating that they contain Classified Information of the Competent Authority of the other Party. The translation shall be placed under the same protection as the originals.

## **Article 9**

### **Destruction of Classified Information**

(1) Classified Information shall be destroyed according to the internal laws of the Parties, in such a manner as to eliminate the partial or total reconstruction of



the same. A report of destruction shall be made and its translation in English shall be delivered to the Competent Security Authority of the Originator. The Originator may expressly prohibit destruction of Classified Information by marking the relevant carrier or sending subsequent written notice. If destruction of the Classified Information is prohibited, it shall be returned to the Competent Authority.

(2) Classified Information marked as **CTΠΟΓΟ CEKPETHO/AKPΩΣ AΠIOPPHTO /TOP SECRET** shall not be destroyed. It shall be returned to the Competent Authority which provided the same.

(3) When it is impossible for one of the Parties to protect and/or return Classified Information generated or transmitted according to this Agreement, the Classified Information shall be destroyed immediately. The Recipient shall notify the Competent Security Authority of the Originator about the destruction of the Classified Information as soon as possible.

## **Article 10**

### **Visits**

(1) Persons arriving on a visit from the State of either Party to the State of the other Party shall be allowed access to Classified Information to the necessary extent as well as to the premises where such Classified Information is handled, processed or stored only after receiving a written permit issued by the Competent Security Authority of the other Party.

(2) The permit referred to in Paragraph 1 shall be granted exclusively to the persons authorised to have access to Classified Information pursuant to the internal laws of the Party delegating such a person.

(3) Request for a visit shall include:

- a. purpose, date and program of the visit;
- b. name and surname of the visitor, date and place of birth, nationality, passport number or identity card number;
- c. position of the visitor together with the name of the institution or organization which he/ she represents;
- d. certification of the level of Personnel Security Clearance held by the visitor;
- e. name and address of the organization to be visited;

f. name, surname and position of the person to be visited.

(4) Visiting procedures shall be agreed between the Competent Security Authorities.

(5) The Competent Security Authorities of the Parties may agree to establish lists of authorized persons to make recurring visits. Further details of the recurring visit are subject to the coordination between Competent Security Authorities.

(6) To the extent required to obtain the permit referred to in Paragraph 1, the personal data of the persons arriving on a visit to the other Party shall be transmitted sufficiently in advance to the Competent Security Authority, in accordance with the internal laws of each Party.

(7) The Competent Security Authorities of both Parties shall ensure the protection of the personal data of the person arriving on a visit pursuant to their internal laws.

(8) Classified Information accessible during the visit shall be protected pursuant to the provisions of this Agreement.

### **Article 11**

#### **Breach of Security Concerning Mutual Protection of Classified Information**

(1) Any breach of security concerning the protection of Classified Information provided or originated as a result of mutual co-operation between the Parties, including this originated in the connection with the performance of a Classified Contract, shall be investigated and prosecuted pursuant to the internal laws of this Party in whose territory the breach has occurred. The Competent Authorities of the Parties shall immediately notify such a case to each other and shall notify the Competent Security Authority of their Party.

(2) In the event of a breach of security of Classified Information which has occurred in the territory of a third country, the Party which provided the information shall take actions referred to in Paragraph 1, if it is legally possible.

(3) The Competent Authority of either Party shall notify immediately the Competent Authority of the other Party in the event of breach of security of



Classified Information and of the result of the actions referred to in Paragraph 1. The other Party shall, upon relevant request, cooperate in the investigation.

## **Article 12**

### **Expenses**

Each Party shall cover its own expenses resulting from the implementation of this Agreement.

## **Article 13**

### **Consultation**

(1) The Competent Security Authorities of the Parties shall consult each other, upon the request of one of them, in order to ensure close cooperation in the implementation of the provisions hereof.

(2) Each Party shall allow the representatives of the Competent Security Authority of the other Party to come on visits to its own territory to discuss the procedures for the protection of Classified Information transmitted by the other Party.

## **Article 14**

### **Settlement of Disputes**

(1) Any disputes concerning the application of this Agreement shall be settled by direct negotiations between the Competent Security Authorities of the Parties, without recourse to outside jurisdiction.

(2) If the settlement of a dispute can not be reached in the manner referred to in Paragraph 1, such a dispute shall be settled through diplomatic channels.

## **Article 15**

### **Final Provisions**

(1) This Agreement shall enter into force in accordance with the internal laws of each of the Parties, which shall be stated in the way of exchange of written notice. The Agreement shall enter into force on the first day of the second

month following the receipt of the latter written notice through diplomatic channels.

(2) This Agreement is concluded for an unlimited period of time. It may be terminated by either Party upon giving a written notice to the other Party. In such a case this Agreement shall expire six months after the date of the termination notice.

(3) In the event of the termination thereof, any Classified Information transmitted or originated as a result of mutual co-operation between the Parties of the Competent Authorities, including Classified Information originated in the connection with performance of Classified Contract, shall continue to be protected pursuant to the provisions of this Agreement as long as required by the Originator.

(4) This Agreement may be amended on the basis of mutual written consent by both Parties. Such amendments shall enter into force in accordance with the provisions of Paragraph 1.

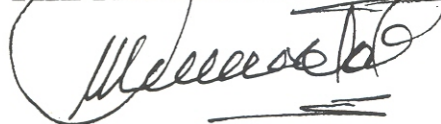
Done at Nicosia on 12 July 2011 in two original sets, each in Bulgarian, Greek and English languages, all texts being equally authentic. In case of divergences of interpretation, the English text shall prevail.

**ON BEHALF OF  
THE GOVERNMENT OF  
THE REPUBLIC OF BULGARIA**



**TSVETA MARKOVA  
CHAIRPERSON OF THE  
STATE COMMISSION ON  
INFORMATION SECURITY**

**ON BEHALF OF  
THE GOVERNMENT OF  
THE REPUBLIC OF CYPRUS**



**COSTAS PAPACOSTAS  
MINISTER OF DEFENCE**