

**AGREEMENT**

**BETWEEN**

**THE GOVERNMENT OF THE REPUBLIC OF  
BULGARIA**

**AND**

**THE GOVERNMENT OF THE GRAND DUCHY OF  
LUXEMBOURG**

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

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

Realising that effective co-operation in political, economic, military, security, intelligence and any other area may require exchange of Classified Information between the Parties,

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

Desiring to create a set of rules regulating the mutual protection of Classified Information exchanged between the Parties under any future co-operation agreements and/or Classified contracts

Have agreed as follows:

## **Article 1**

### **Objective and scope**

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

(2) This Agreement shall be applicable to any activities, contracts or agreements involving Classified Information that will be conducted or concluded between the Parties in the future.

(3) The provisions of this Agreement shall also apply to the Classified Information already generated or exchanged in the process of cooperation between the Parties before entering into force of this Agreement.

## **Article 2**

### **Definitions**

For the purpose of this Agreement:

(1) **"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 national laws and regulations, requires protection against unauthorised access.

(2) **"Security classification level"** means 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.

(3) **"Personnel Security Clearance"** means determination, issued by the respective national authority as a result of a vetting procedure, which ascertains that a certain individual may be granted access to Classified Information in accordance with the national laws and regulations.

(4) **"Facility Security Clearance"** means determination, issued by the respective national authority as a result of a vetting procedure, which ascertains that, on the matters of security, a certain legal entity meets the physical and organisational requirements for generation, process and storing of Classified Information in accordance with the national laws and regulations.

(5) **"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.

(6) **"Competent Authority"** means the national authority, which in compliance with the national laws and regulations of the respective 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 3 of this Agreement.

(7) **"Originating Party"** means the Party which transmits Classified Information.

(8) **"Receiving Party"** means the Party to which Classified Information is transmitted.

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

(10) **"Classified Contract"** means an agreement between two or more Contractors which contains Classified Information or requires access to Classified Information.

(11) **"Contractor"** means an individual or a legal entity possessing the legal capacity to conclude contracts and/or is a party to a classified contract.

(12) **"Sub-contractor"** means a Contractor to whom a prime Contractor lets a sub-contract.

(13) **"Breach of security"** means an act or an omission contrary to the national laws and regulations, which results or may result in an unauthorised access of Classified Information.

(14) **"Unauthorised access of Classified Information"** means 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 Personnel Security

Clearance/Facility Security Clearance and who does not have “the need to know”.

### **Article 3 Competent Authorities**

The Competent Authorities of the Parties are:

**For the Republic of Bulgaria:**

- State Commission on Information Security;

**For the Grand Duchy of Luxembourg:**

- Service de renseignement de l'État  
Autorité nationale de Sécurité (National Security Authority)

### **Article 4 Security Classification Levels**

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 of the respective Party:

<b>For the Republic of Bulgaria</b>	<b>Equivalent in English</b>	<b>For the Grand Duchy of Luxembourg</b>
СТРОГО СЕКРЕТНО	TOP SECRET	TRES SECRET LUX
СЕКРЕТНО	SECRET	SECRET LUX
ПОВЕРИТЕЛНО	CONFIDENTIAL	CONFIDENTIEL LUX
ЗА СЛУЖЕБНО ПОЛЗВАНЕ	RESTRICTED	RESTREINT LUX

## **Article 5**

### **Measures for the protection of Classified Information**

(1) In compliance with their national laws and regulations, the Parties shall implement all appropriate measures for protection of Classified Information, which is commonly generated or exchanged under this Agreement. 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 Security classification level of the mutually generated Classified Information under this Agreement, is defined by mutual consent of the Parties.

(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.

(4) Classified Information shall only be made accessible to individuals who are authorized in accordance with national laws and regulations to have access to Classified Information of the equivalent security classification level and who have a Need-to-know and who have been briefed accordingly.

(5) The Receiving Party is obligated:

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

b) to grant Classified Information a security classification level equivalent to that provided by the Originating Party;

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

(6) If any other Agreement concluded between the Parties contains stricter regulations regarding the exchange or protection of Classified Information, these regulations shall apply.

## **Article 6**

### **Security Co-operation**

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

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

(3) 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 and practices for protection of Classified Information, applied by the respective Party.

(4) On request, the Competent Authorities, in accordance with their national laws and regulations, assist each other throughout the procedures for issuance of a Personnel Security Clearance and Facility Security Clearance.

(5) The Parties mutually recognize their Personnel Security Clearances and Facility Security Clearances, in accordance with their national laws and regulations.

(6) Within the scope of this Agreement, the Competent Authorities shall inform each other without delay about revocation of Personnel and Facility Security Clearances or the alteration of the security classification level.

(7) The Security and Intelligence Services of the Parties may directly exchange Classified Information in accordance with national laws and regulations.

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

## **Article 7**

### **Transfer of Classified Information**

(1) Classified Information shall be transferred by means of diplomatic or military couriers or by other means, approved in advance by the Competent Authorities in accordance with national laws and regulations.

(2) Electronic transmission of Classified Information shall be carried out through certified cryptographic means in accordance with national laws and regulations.

(3) If transferred Classified Information is marked CEKPETHO /SECRET/ SECRET LUX and above, the Receiving Party shall confirm the receipt in writing. The receipt of other Classified Information shall be confirmed on request.

## **Article 8**

### **Translation, reproduction, destruction of Classified Information.**

#### **Changing and removing of Security classification level.**

(1) Classified Information with a security classification level CTPOFO CEKPETHO / TOP SECRET / TRES SECRET LUX 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 have a security clearance up to the appropriate security classification level. Such translations shall bear an equal security classification level in accordance with Article 4 of this Agreement.

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

(4) When Classified Information is reproduced, the security classification level of the original 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.

(5) The Receiving Party shall not change and/or remove the security classification level of the received Classified Information without prior written permission of the Originating Party.

(6) Classified Information shall be destroyed insofar as to prevent its reconstruction in whole or in part in accordance with national laws and regulations.

(7) The Originating Party may explicitly prohibit the reproduction or destruction of Classified Information by marking the relevant carrier of Classified Information or sending subsequent written notice. If destruction of the Classified Information is prohibited, it shall be returned to the Originating Party.

(8) Classified Information of СТОГО СЕКРЕТО / TOP SECRET / TRES SECRET LUX security classification level shall not be destroyed. It shall be returned to the Originating Party.

(9) Information classified as СЕКРЕТО/SECRET/SECRET LUX shall be destroyed in accordance with the national laws and regulations after it is no longer considered necessary by the Receiving Party.

(10) In case of a crisis situation which makes it impossible to protect and return Classified Information, generated or transferred according to this Agreement, the Classified Information shall be destroyed immediately. The Receiving Party shall notify the Competent Authority of the Originating Party in writing about the destruction of the Classified Information as soon as possible.

## **Article 9**

### **Classified Contracts**

(1) Classified Contracts shall be concluded and implemented in accordance with national laws and regulations.

(2) Upon request the Competent Authority of the Receiving Party shall confirm that a proposed Contractor has been issued an appropriate Personnel or Facility Security Clearance. If the proposed Contractor does not hold an appropriate security clearance, the Competent Authority of the Originating Party may request the Competent Authority of the Receiving Party to issue the appropriate security clearance.

(3) The Competent Authority in which state's territory the Classified Contract is to be performed, shall assume the 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. Periodical security inspections may be carried out in accordance with national laws and regulations.

(4) The Contractor shall be obliged to:

a) hold a Facility Security Clearance at the appropriate security classification level;

b) ensure that the individuals requiring access to Classified Information hold a Personnel Security Clearance at the appropriate security classification level;

c) ensure that all individuals, granted access to Classified Information, are informed of their responsibilities to protect Classified Information in accordance with national laws and regulations;

d) perform periodic security inspections of its premises.

(5) Sub-contractors engaged in Classified Contracts shall comply with the security requirements applied to the Contractors.

(6) Every Classified Contract concluded in accordance with this Agreement shall include an appropriate security annex which is an integral part of the Classified Contract identifying the following aspects:

a) a classification guide;

b) a procedure for the communication of changes in the security classification level of the information;

c) communication channels and means for electromagnetic transmission;

d) procedures for the transportation of Classified Information;

e) contact details of the Competent Authorities responsible for the co-ordination of the protection of Classified Information related to the Contract;

f) an obligation to notify any actual or suspected Breach of Security.

(7) A copy of the security annex of all Classified Contracts shall be forwarded to the Competent Authority of the Party where the Classified Contract is to be performed, to allow an adequate supervision and control of the security standards, procedures and practices established by the Contractors for the protection of Classified Information.

(8) Representatives of the Competent Authorities may visit each other in order to analyse the efficiency of the measures adopted by a Contractor for the protection of the Classified Information involved in a Classified Contract. Notice of the visit shall be provided, at least, three (3) weeks in advance.

## **Article 10**

### **Visits**

(1) Visits that involve access to Classified Information shall be subject to prior permission by the Competent Authority of the host Party.

(2) The request for visit shall be submitted at least 3 weeks prior to the visit and shall contain:

- a) visitor's name and surname, date and place of birth, nationality;
- b) passport number or another identification card number of the visitor;
- c) position of the visitor and name of the organization represented;
- d) level of the Personnel Security Clearance of the visitor, if applicable;
- e) purpose, proposed working program and planned date of the visit;
- f) names of organizations and facilities requested to be visited;
- g) number of visits and period required;
- h) contact details of the Security Officers of the facilities;
- i) other data, agreed upon by the Competent Authorities.

(3) For the implementation of this Agreement recurring visits may be executed. The Competent Authorities of the Parties approve a list of authorised individuals to make recurring visits. Those lists are valid for an initial period of twelve months. Once the lists have been approved by the Competent Authorities of the Parties, the terms of the concrete visits shall be directly arranged with the Security Officers of the facilities to be visited by the individuals.

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

## **Article 11**

### **Breach of Security**

(1) The Competent Authority of the Receiving Party shall immediately notify the Competent Authority of the Originating Party of any suspicion or discovery of a Breach of Security.

(2) The Competent Authority of the Receiving Party shall undertake all possible appropriate measures in accordance with its national laws and regulations so as to limit the consequences of the Breach of Security and to prevent further violations and ensure the appropriate investigation. On request,

the Competent Authority of the Originating Party shall provide investigative assistance. The Competent Authority of the Receiving Party shall inform in writing the Competent Authority of the Originating Party of the outcome of the proceedings and the corrective measures undertaken due to the violation.

(3) If a Breach of security occurs in a third country, the Competent Authority of the dispatching Party shall take the actions under paragraph 2, where possible.

## **Article 12**

### **Costs**

Each Party shall bear the costs incurred in the course of implementing its obligations under this Agreement.

## **Article 13**

### **Settlement of Disputes**

Any dispute regarding the interpretation or application of this Agreement shall be settled by consultations and negotiations between the Parties.

## **Article 14**

### **Final Provisions**

(1) This Agreement shall enter into force on the first day of the second month after the date of the receipt of the latest written notification by which the Parties have notified each other, through diplomatic channels, that their national legal requirements necessary for its entry into force have been fulfilled.

(2) This Agreement may be amended by mutual written consent of the Parties. The amendments shall be the integral part of this Agreement. Such amendments shall enter into force in accordance with the provision of paragraph 1 of this Article.

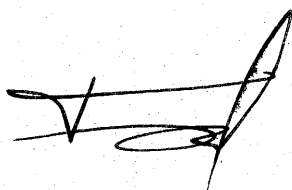
(3) This Agreement is concluded for an indefinite period of time. Either Party may denounce this Agreement by giving the other Party written notice through diplomatic channels. In that case, this Agreement shall terminate six months from the date on which the other Party has received the denunciation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

(4) In case of termination of this Agreement, all Classified Information exchanged 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.

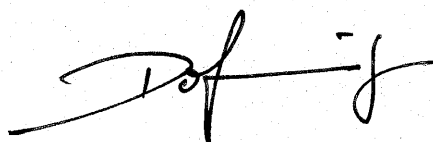
Done at Sofia on 29 January 2018 in 2 original copies, each in the Bulgarian, French and English languages, all texts being equally authentic. In case of any divergence of interpretation, the English text shall prevail.

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



**Boris Dimitrov  
Chairperson of the State  
Commission on Information  
Security**

**For the Government of the  
Grand Duchy of Luxembourg**



**Ronald Dofing  
Ambassador of the  
Grand Duchy of Luxembourg  
to the Republic of Bulgaria**