

**AGREEMENT BETWEEN THE GOVERNMENT OF THE REPUBLIC OF  
SERBIA AND THE GOVERNMENT OF THE GRAND-DUCHY OF  
LUXEMBOURG ON THE EXCHANGE AND MUTUAL PROTECTION OF  
CLASSIFIED INFORMATION**

**The Government of the Republic of Serbia  
and  
The Government of the Grand-Duchy of Luxembourg**

(hereinafter referred to as: “the Parties”),

Recognizing the need to set rules on protection of Classified Information mutually exchanged within the scope of political, military, security, economic, legal, scientific and technological or any other cooperation, as well as Classified Information generated in the process of such cooperation,

Intending to ensure the mutual protection of all Classified Information that has been classified by one Party and transferred to the other Party, or jointly generated in the course of co-operation between the Parties,

Desiring to establish a set of rules on the mutual protection of Classified Information to be generated or exchanged between the Parties,

Considering the mutual interests in the protection of Classified Information, in accordance with national laws and regulations of the Parties,

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 jointly generated or exchanged between the Parties.
2. This Agreement shall be applicable to any activities, contracts or agreements involving Classified Information to be conducted or concluded between the Parties in the future.

**Article 2  
Definitions**

For the purposes of this Agreement:

- a) “Breach of Security” means an act or an omission which is contrary to this Agreement or the national legislation of the Parties, the result of which may lead to disclosure, loss, destruction, misappropriation or any other type of compromise of Classified Information;
- b) “Classified Contract” means an agreement between two or more Contractors or Subcontractors, which contains Classified Information or the implementation of which requires access to Classified Information;
- c) “Classified Information” means any information, regardless of its form, which is transmitted or generated between the Parties in accordance with national laws and regulations of either Party, which requires protection against unauthorized disclosure, misappropriation or loss and is designated as such;
- d) “Competent Authority” means National Security Authority and any other competent entity which, in accordance with national laws and regulations, is responsible for the supervision of the implementation of this Agreement as referred to in Article 4, Paragraph 1 of this Agreement;
- e) “Contractor” means an individual or a legal entity possessing the legal capacity to conclude Classified Contracts;
- f) „Facility Security Clearance” means the determination by the Competent Authority confirming, in accordance with national laws and regulations that the Contractor or Subcontractor meets the physical and organizational capability to handle and store Classified Information up to a certain security classification level;
- g) “Need-to-know” means the necessity to have access to specific Classified Information in the scope of given official duties and/or for the performance of a specific task;
- h) “Originating Party” means the Party, including any entity which provides Classified Information in accordance with national laws and regulations;
- i) “Personnel Security Clearance” means the determination by the Competent Authority confirming, in accordance with national laws and regulations that the individual is eligible to have access to Classified Information up to a certain security classification level;
- j) “Receiving Party” means the Party, including any entity to which Classified Information of the Originating Party is transmitted;
- k) “Sub-contractor” means a Contractor to whom a prime Contractor lets a sub-contract;

- 1) "Third Party" means any state, organization, legal entity or individual, which is not a party to this Agreement;

**Article 3**  
**Security Classification Levels**

The Parties agree that the following security classification levels and markings are equivalent and that they correspond to the security classification levels specified in their national legislation:

For the Republic of Serbia	For the Grand-Duchy of Luxembourg	Equivalent in English
ДРЖАВНА ТАЈНА	TRÈS SECRET LUX	TOP SECRET
СТРОГО ПОВЕРЉИВО	SECRET LUX	SECRET
ПОВЕРЉИВО	CONFIDENTIEL LUX	CONFIDENTIAL
ИНТЕРНО	RESTREINT LUX	RESTRICTED

**Article 4**  
**Competent Authorities**

1. The Competent Authorities of the Parties are:

For the Government of the Republic of Serbia:

Канцеларија Савета за националну безбедност и заштиту тајних података

For the Government of the Grand-Duchy of Luxembourg:

Service de renseignement de l'Etat

Autorité nationale de Sécurité

2. The Parties shall inform each other through diplomatic channels about any changes or modifications regarding their Competent Authorities.
3. The competent authorities shall inform each other of the laws and regulations in force in their states as well as any changes thereof affecting the protection of Classified Information generated or exchanged in accordance with this Agreement.

4. In order to achieve and maintain comparable standards of security, the Competent Authorities may provide each other with information about any security standards, procedures and practices for the protection of Classified Information employed by the respective Party.

#### **Article 5**

##### **Measures for the protection and the access to Classified Information**

1. In accordance with their national laws and regulations, the Parties shall take all appropriate measures for the prevention of Classified Information, which is exchanged or generated under this Agreement. The same level of protection shall be ensured for such Classified Information as it is provided for the national Classified Information of the equivalent security classification level in accordance with Article 3 of this Agreement.

2. The Originating Party shall inform the Receiving Party in writing about any change of the security classification level of the transmitted Classified Information in order to apply the appropriate protection measures.

3. 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 have a Need-to-know and who have been briefed accordingly.

4. Within the scope of this Agreement each Party shall recognize as equivalent the Personnel Security Clearances and Facility Security Clearances issued by the other Party in accordance with national laws and regulations.

5. The Competent Authorities shall, in accordance with national laws and regulations, assist each other upon request in carrying out vetting procedures necessary for the application of this Agreement.

6. Within the scope of this Agreement, the Competent Authorities of the Parties shall inform each other without delay about any alteration with regard to Personnel and Facility Security Clearances, in particular about their withdrawal or downgrading.

7. Upon request of the Competent Authority of the Originating Party, the Competent Authority of the Receiving Party shall issue a written confirmation that an individual has been issued a Personnel Security Clearance or a legal entity has been issued a Facility Security Clearance.

8. The Receiving Party shall:

- a) not disclose Classified Information to any Third Party without a prior written consent of the Originating Party issued in accordance with national laws and regulations;
- b) mark the received Classified Information in accordance with the equivalence set forth in Article 3;
- c) not declassify or downgrade the provided Classified Information without a prior written consent of the Originating Party;
- d) use Classified Information solely for the purposes it has been provided for.

**Article 6**  
**Transmission of Classified Information**

1. Classified Information shall be transmitted through diplomatic or military channels unless otherwise approved by the Competent Authorities in accordance with national laws and regulations. The Receiving Party shall confirm the receipt of Classified Information in writing.
2. Electronic transmission of Classified Information shall be carried out through certified cryptographic means agreed by the Competent Authorities in accordance with national laws and regulations.
3. The intelligence, security and police services of the Parties may, in accordance with national laws and regulations, exchange operational and/or intelligence information directly between each other.

**Article 7**  
**Reproduction and Translation of Classified Information**

1. Translations and reproductions of Classified Information shall be made in accordance with national laws and regulations of the Receiving Party and the following procedures:
  - a) translations and reproductions shall be marked and protected as original Classified Information;
  - b) translations and the number of copies shall be limited to that required for official purposes;
  - c) translations shall bear an appropriate note in the language of the translation, indicating that it contains Classified Information received from the Originating Party.

2. Classified Information marked СТРОГО ПОВЕРЉИВО / SECRET LUX / SECRET or above shall be translated or reproduced only upon a prior written consent of the Originating Party.

#### **Article 8**

##### **Destruction of Classified Information**

1. Classified Information shall be destroyed in a manner that prevents its partial or total reconstruction.
2. Classified Information marked up to СТРОГО ПОВЕРЉИВО/SECRET LUX/ SECRET shall be destroyed in accordance with national laws and regulations.
3. A report on destruction of Classified Information shall be made and its English translation shall be delivered to the Competent Authority of the Originating Party.
4. Classified Information marked ДРЖАВНА ТАЈНА / TRÈS SECRET LUX/ TOP SECRET shall not be destroyed, except in cases referred to in paragraph 5 of this Article. It shall be returned to the Competent Authority of the Originating Party.
5. In case of a crisis situation in which it is impossible to protect or return Classified Information, it shall be destroyed immediately. The Receiving Party shall inform the Competent Authority of the Originating Party about this destruction 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 National Security Authority of the Originating Party may request the Competent Authority of the Receiving Party to issue the appropriate security clearance.
3. The Competent Security Authority in the state territory of which 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 by the Competent Security Authorities.
4. A security annex shall be an integral part of each Classified Contract or sub-contract by which the Originating Party shall specify which Classified Information is to be released to the Receiving

Party, which security classification level has been assigned to that information and the Contractor's obligations to protect the Classified Information. Subcontracting must be explicitly allowed in the security annex of the Classified Contract. A copy of the security annex shall be sent to the Competent Authority of the Originating Party.

5. Prior to release to either Party's Contractors or prospective Contractors of any Classified Information received from the other Party, the Receiving Party shall, in accordance with its national laws and regulations, ensure that Contractors or prospective Contractors can afford adequate security protection to Classified Information and:

- a) perform an appropriate Facility Security Clearance procedure of the Contractors and Subcontractors;
- b) perform an appropriate Personnel Security Clearance procedure for all personnel whose duties require access to Classified Information;
- c) ensure that all persons having access to Classified Information are informed of their responsibilities;
- d) carry out periodic security inspections of relevant security-cleared facilities.

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

7. Representatives of the Competent Authorities may visit each other in order to analyze the efficiency of the measures adopted by a Contractor for the protection of Classified Information involved in a Classified Contract.

## **Article 10**

### **Visits**

1. Visits related to Classified Contracts and involving access to Classified Information are subject to prior written approval given by the Competent Authority of the host Party.

2. The Competent Authority of the host Party shall receive a request for visit at least three (3) weeks in advance.

3. In urgent cases, the request for visit can be transmitted in shorter time.

4. The request for visit shall include:

- a) visitor's name and surname, place and date of birth, citizenship, passport or identification document number;

- b) name of the legal entity represented by the visitor and position of the visitor in the legal entity;
- c) name, address and contact information of the legal entity to be visited;
- d) information on the visitor's Personnel Security Clearance, its validity and level;
- e) object and purpose of the visit;
- f) expected date and duration of the requested visit. In case of recurring visits the total period covered by the visits shall be stated;
- g) date, signature and the official seal of the Competent Authority.

5. Once the visit has been approved the Competent Authority of the host Party shall provide a copy of the request for visit to the security officers of the legal entity to be visited.

6. The validity of visit approvals shall not exceed one year.

7. The competent Authorities of the Parties may draw up lists of individuals authorized to make recurring visits. The lists are valid for an initial period of twelve months. The terms of the respective visits shall be directly arranged with the appropriate points of contact in the legal entity to be visited by these individuals, in accordance with the terms and conditions agreed upon.

8. 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. In case of any suspicion or discovery of a Breach of Security the Competent Authority of the Receiving Party shall inform the Competent Authority of the Originating Party immediately, and initiate an appropriate investigation.
2. If a breach of security arises in a third state, the Competent Authority of the Originating Party shall take all necessary measures in order to ensure that the actions prescribed in Paragraph 1 are initiated.
3. The Originating Party shall, upon request, co-operate in the investigation in accordance with Paragraph 1.
4. The Originating Party shall be informed of the results of the investigation and shall receive the final report on the reasons and extent of the damage.

**Article 12**  
**Expenses**

Each Party shall bear its own expenses incurred in the course of implementation and supervision of this Agreement.

**Article 13**  
**Settlements of disputes**

Any dispute regarding the interpretation or application of this Agreement shall be settled by consultations and negotiations between the Parties. During the negotiations both Parties shall continue to fulfill all other obligations under the Agreement.


**Article 14**  
**Final Provisions**

1. This Agreement is concluded for an indefinite period of time and enters into force on the first day of the second month after the date of 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.

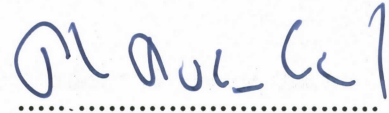
2. This Agreement may be amended any time on the basis of mutual written approval of the Parties. The amendments shall enter into force in accordance with Paragraph 1.
3. Each Party may, at any time, terminate this Agreement by written notification to the other Party, through diplomatic channels. In this case, the termination takes effect six months after the date of receipt of the respective notification.
4. Notwithstanding the termination of this Agreement, the Parties shall ensure that all Classified Information shall continue to be protected until the Originating Party dispenses the Receiving Party from this obligation.

Done at LUXEMBOURG on 04.02.2020 in two original sets, each in the Serbian, 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 Serbia**

  
.....

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

  
.....