

**AGREEMENT  
BETWEEN  
THE GOVERNMENT OF THE REPUBLIC OF CROATIA  
AND  
THE GOVERNMENT OF THE REPUBLIC OF MACEDONIA  
ON EXCHANGE AND MUTUAL PROTECTION OF CLASSIFIED INFORMATION**

The Government of the Republic of Croatia and the Government of the Republic of Macedonia (hereinafter referred to as “the Parties”),

In line with the bilateral and multilateral agreements already signed on political and security-related issues and on enhancing the political, military and economic cooperation,

Having agreed to hold talks on political and security-related issues and to broaden and tighten their mutual co-operation,

Being aware of the changes in the political 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 Parties,

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

Have agreed as follows:

**Article 1  
Objective**

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

**Article 2  
Definitions**

For the purposes of this Agreement:

- (1) “**Classified Information**” means any information irrespective of its form, including objects and facilities or any parts thereof, which require protection against unauthorized access, in accordance with national laws and regulations;
- (2) “**Need-to-know**” means the need to have access to Classified Information in the scope of a given official position and for the performance of a specific task;
- (3) “**Unauthorised access to Classified Information**” means any form of disclosure, misuse, damage, submission, destruction, loss or any action resulting in breach of security of Classified Information;
- (4) “**Security classification level**” means category, in accordance with the national laws and regulations, which characterises the importance of Classified Information, level of restriction of access to it and level of its protection by the Parties;
- (5) “**Classification marking**” means a mark on any Classified Information, which shows the security classification level;
- (6) “**Originating Party**” means the Party that originates or transmits the Classified Information to the Receiving Party;
- (7) “**Receiving Party**” means the Party to which Classified Information is transmitted;

- (8) “**Competent Security Authority**” means the main authority, which in accordance with the national laws and regulations of the respective Party performs the national policy for the protection of Classified Information, exercises overall control in this sphere as well as conducts the implementation of this Agreement;
- (9) “**Contractor**” means an individual or a legal entity possessing the legal capacity to conclude contracts or a party to a Classified Contract under the provisions of this Agreement;
- (10) “**Classified Contract**” means an agreement between two or more Contractors, which contains or provides access to Classified Information;
- (11) “**Personnel Security Clearance Certificate**” means a positive determination granted by the Competent Security Authority in accordance with the national laws and regulations, confirming that the individual is security cleared for access to Classified Information;
- (12) “**Facility Security Clearance Certificate**” means a positive determination granted by the Competent Security Authority in accordance with the national laws and regulations, confirming that the legal entity is security cleared for access to Classified Information;
- (13) “**Third Party**” means any state, organisation, legal entity and individual which is not a party to this Agreement.

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

The 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 Party:

For the Republic of Croatia	For the Republic of Macedonia	Equivalent in English
VRLO TAJNO	ДРЖАВНА ТАЈНА	TOP SECRET
TAJNO	СТРОГО ДОВЕРЛИВО	SECRET
POVJERLJIVO	ДОВЕРЛИВО	CONFIDENTIAL
OGRANIČENO	ИНТЕРНО	RESTRICTED

### **Article 4 Competent Security Authorities**

1. The Competent Security Authorities of the Parties are:
  - For the Republic of Croatia:  
Office of the National Security Council
  - For the Republic of Macedonia:  
Directorate for Security of Classified Information
2. The Competent Security Authorities shall inform each other of the national laws and regulations in force regulating the protection of Classified Information and shall exchange information about the security standards, procedures and practices for the protection of Classified Information.
3. In order to ensure close co-operation in the implementation of this Agreement, the Competent Security Authorities may hold consultations.

**Article 5**  
**National Measures and Access to Classified Information**

1. In accordance with their national laws and regulations, the Parties shall implement all appropriate measures for the protection of Classified Information, which is exchanged 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 as defined in 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 released Classified Information, in order to apply the appropriate security measures.
3. Access to Classified Information shall be granted only on the basis of Personnel or Facility Security Clearance Certificate issued in accordance with the national laws and regulations of the Parties.
4. The Receiving Party shall:
  - a) submit Classified Information to a Third Party only upon prior written consent of the Originating Party;
  - b) grant Classified Information a security classification level equivalent to that provided by the Originating Party;
  - c) use Classified Information only for the purposes it has been provided for.
5. 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**  
**Transmission of Classified Information**

1. Classified Information shall be transmitted through diplomatic channels or by military and other courier services approved by the Competent Security Authorities of the Parties. The Receiving Party shall confirm the receipt of Classified Information in writing.
2. If a large consignment, containing Classified Information, is to be transmitted, the Competent Security Authorities shall mutually agree and approve in writing the means of transportation, the route and security measures on case-by-case basis.
3. The Parties shall transmit Classified Information by other approved means of transmission in accordance with the security procedures agreed upon by the Competent Security Authorities.
4. If necessary, the security and intelligence services of the Parties may exchange Classified Information within their scope of work directly to each other.

**Article 7**  
**Marking of Classified Information**

1. The Receiving Party shall mark the received Classified Information in accordance with the national laws and regulations.
2. Copies and translations of the received Classified Information shall be marked and handled in the same manner as the originals.

**Article 8**  
**Reproduction and Translation of Classified Information**

1. Information classified as TOP SECRET shall be translated or reproduced only in exceptional cases upon prior written permission of the Originating Party.
2. All reproduced copies of Classified Information shall be marked with the original classification marking. Such reproduced information shall be placed under the same control as the original information. The number of copies shall be restricted to that required for official purposes.
3. All translations of Classified Information shall be made by security cleared individuals. The translation shall be marked with the original classification marking and shall bear an appropriate note in the language into which it is translated that the translation contains Classified Information of the Originating Party.

**Article 9**  
**Destruction of Classified Information**

1. Classified Information shall be destroyed in such a manner as to eliminate the possibility of its partial or total reconstruction.
2. Information classified as TOP SECRET shall not be destroyed. It shall be returned to the Originating Party.
3. The Originating Party may by additional marking or sending subsequent written notice expressly prohibit reproduction, alteration or destruction of Classified Information. If destruction of Classified Information is prohibited, it shall be returned to the Originating Party.
4. In case of a crisis situation, Classified Information, impossible to be protected or returned to the Originating Party, shall be destroyed immediately. The Receiving Party shall notify the Originating Party in writing about the destruction of Classified Information.

**Article 10**  
**Classified Contracts**

1. Classified Contracts shall be concluded and implemented in accordance with the national laws and regulations of each Party. Upon request the Competent Security Authority of each Party shall furnish confirmation that a proposed Contractor has been issued an appropriate national Facility Security Clearance Certificate. If the proposed Contractor does not hold the appropriate Facility Security Clearance Certificate the Competent Security Authority of each Party may request for that Contractor to be security cleared.
2. A security annex shall be an integral part of each Classified Contract or sub-contract by which the Contractor of the Originating Party shall specify which Classified Information is to be released to the Receiving Party, and which security classification level has been assigned to this information.
3. The Contractor's obligations to protect the Classified Information shall refer, at least, to the following:
  - a) disclosure of Classified Information exclusively to persons who have been previously issued the appropriate Personnel Security Clearance Certificate, who have "need-to-know" and who are engaged in the carrying out of the Classified Contract;
  - b) transmission of Classified Information by the means in accordance with the provisions of this Agreement;
  - c) the procedures and mechanisms for communicating any changes that may arise in respect of Classified Information;

- d) usage of Classified Information under the Classified Contract only for the purposes related to the subject of the contract;
  - e) strict adherence to the provisions of this Agreement related to the procedures for handling of Classified Information;
  - f) the obligation to notify the Contractor's Competent Security Authority of any actual, attempted or suspected unauthorised access to Classified Information related to the Classified Contract in accordance with the provisions of this Agreement;
  - g) release of Classified Information related to the Classified Contract to any Third Party only with the prior written consent of the Originating Party.
4. The measures required for the protection of 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 detail in the respective Classified Contract.
5. Classified Contracts of security classification level RESTRICTED shall contain an appropriate security clause identifying the minimum security measures to be applied for the protection of Classified Information. For such contracts the Contractors shall be security briefed in accordance with the national laws and regulations.

#### **Article 11 Visits**

1. The Competent Security Authorities shall hold consultations to discuss the procedures for protection of Classified Information.
2. The Competent Security Authority of the host Party shall, upon request of the Competent Security Authority of the visiting Party, allow access to Classified Information or to premises where Classified Information is handled to the visitors in accordance with the national laws and regulations.
3. The request referred to in paragraph 2 of this Article shall include:
- a) visitor's name, 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 organisation represented;
  - d) appropriate security clearance certificate of the visitor;
  - e) purpose, proposed working program and planned date of the visit;
  - f) names of organisations and facilities to be visited;
  - g) number of visits and period required;
  - h) other data, if agreed upon by the Competent Security Authorities.
4. Each Party shall guarantee the protection of personal data of the visitors in accordance with its national laws and regulations.

#### **Article 12 Breaches of Security**

1. In case of actual or suspected breach of security, the Competent Security Authority of the Party where it has occurred shall, without delay, inform the Originating Party and, in accordance with the national laws and regulations, initiate appropriate proceedings, in order to determine the circumstances of the breach. The results of the proceedings shall be forwarded to the Originating Party.

2. When the breach of security has occurred in a Third Party, the Competent Security Authority of the sending Party shall take the actions referred to in paragraph 1 of this Article without delay.

### **Article 13 Expenses**

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

### **Article 14 Settlement of Disputes**

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

### **Article 15 Final Provisions**

1. This Agreement shall enter into force on 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 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 notice in writing through diplomatic channels. In that case, this Agreement shall terminate six (6) 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.

Done at \_\_\_\_\_ on \_\_\_\_\_ in two originals, each in the Croatian, Macedonian 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 CROATIA**

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