

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

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

Considering that the Parties co-operate in matters such as, but not limited to, foreign affairs, defence, security, police, and science, industry and technology,

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

Desiring to establish a set of rules regulating the mutual protection of Classified Information generated or exchanged between the Parties, or public or private legal entities or individuals under the jurisdiction of the Parties,

Have agreed as follows:

**Article 1**

**Objective**

The objective of this Agreement is to ensure the 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 form, which requires protection against Security Breach and has been classified in accordance with national laws and regulations of the Originating Party;
- (2) “**Need-to-Know**” means the necessity to have access to Classified Information in the scope of a given official position and for the performance of a specific task;

- (3) **“Security Breach”** means any form of unauthorized disclosure or alteration, misuse, damage or destruction of Classified Information, as well as any other action or inaction which may result in loss of its confidentiality, integrity or availability;
- (4) **“Security Classification Level”** means a category which, in accordance with national laws and regulations, characterises the level of restriction of access to Classified Information and the minimum level of its protection by the Parties;
- (5) **“Originating Party”** means the Party which provides Classified Information or under whose authority Classified Information is generated;
- (6) **“Receiving Party”** means the Party, as well as any public or private legal entity or individual under its jurisdiction, to which Classified Information of the Originating Party is transmitted;
- (7) **“National Security Authority”** means the national authority responsible for the implementation and supervision of this Agreement;
- (8) **“Competent Security Authority”** means the National Security Authority, Designated Security Authority or National Communications Security Authority or another national authority which, in accordance with national laws and regulations, implements this Agreement;
- (9) **“Contractor”** means an individual or a legal entity possessing the legal capacity to conclude contracts;
- (10) **“Classified Contract”** means an agreement between two or more Contractors which involves or the execution of which requires access to Classified Information;
- (11) **“Personnel Security Clearance”** means determination by the Competent Security Authority confirming, in accordance with its national laws and regulations, that an individual is eligible to have access to Classified Information;
- (12) **“Facility Security Clearance”** means determination by the Competent Security Authority confirming, in accordance with its national laws and regulations, that a legal entity or individual meets the conditions for access to and handling of Classified Information;
- (13) **“Third Party”** means any state, organization, legal entity or individual which is not a party to this Agreement.

### **Article 3**

#### **Security Classification Levels**

1. Any Classified Information provided under this Agreement shall be marked with the appropriate Security Classification Level in accordance with national laws and regulations of the Parties.

2. The Parties agree that the following Security Classification Levels are equivalent to each other:

| For the Republic of Croatia | Equivalent in English | For the Republic of Finland                |
|-----------------------------|-----------------------|--|
| VRLO TAJNO                  | TOP SECRET            | ERITTÄIN SALAINEN or<br>YTTERST HEMLIG     |
| TAJNO                       | SECRET                | SALAINEN or HEMLIG                         |
| POVJERLJIVO                 | CONFIDENTIAL          | LUOTTAMUKSELLINEN<br>or KONFIDENTIELL      |
| OGRANIČENO                  | RESTRICTED            | KÄYTTÖ RAJOITETTU or<br>BEGRÄNSAD TILLGÅNG |

3. The Receiving Party shall ensure that the classifications of the information are not altered or revoked, except as authorised in writing by the Originating Party.

#### **Article 4**

##### **Competent Security Authorities**

1. The National Security Authorities of the Parties are:

For the Republic of Croatia:

- Office of the National Security Council;

For the Republic of Finland:

- Ministry for Foreign Affairs.

2. The Parties shall inform each other through diplomatic channels of any changes of the National Security Authorities. The National Security Authorities shall inform each other of any other Competent Security Authorities and any subsequent changes of these authorities.

3. The National Security Authorities shall inform each other of the national laws and regulations in force regulating the protection of Classified Information and shall, on request, exchange information about the security standards, procedures and practices for the protection of Classified Information.

#### **Article 5**

##### **Protection Measures and Access to Classified Information**

1. In accordance with their national laws and regulations, the Parties shall take all appropriate measures for the protection of Classified Information generated or exchanged under this Agreement. The same level of protection shall be ensured for such Classified Information as is provided to the national Classified Information of the equivalent 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 that the latter apply the appropriate security measures.

3. Access to Classified Information shall only be granted to individuals who have a Need-to-Know, who have been issued an appropriate Personnel Security Clearance in accordance with the national laws and regulations and who have been briefed on their responsibilities for the protection of Classified Information.

4. A Personnel Security Clearance is not required for access to Classified Information at the OGRANIČENO / KÄYTTÖ RAJOITETTU or BEGRÄNSAD TILLGÅNG level.

5. Within the scope of this Agreement, each Party shall recognize the Personnel and Facility Security Clearances issued by the other Party.

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

7. Within the scope of this Agreement, the National Security Authorities shall inform each other without delay about any alteration with regard to Personnel and Facility Security Clearances, in particular about the revocation or the alteration of Security Classification Levels.

8. Upon request of the National Security Authority of the Originating Party, the National Security Authority of the Receiving Party shall issue a written confirmation that an individual has the right to access Classified Information or a legal entity has been issued a Facility Security Clearance.

9. The Receiving Party shall:

- a) submit Classified Information to a Third Party only upon prior written consent of the Originating Party;
- b) mark the received Classified Information in accordance with the Security Classification Level equivalence set forth in Article 3;
- c) use Classified Information only for the purposes that it has been provided for.

10. If any other agreement concluded between the Parties contains stricter regulations regarding the exchange or protection of Classified Information, these stricter regulations shall apply.

## **Article 6**

### **Transmission of Classified Information**

1. Classified Information shall be transmitted through channels mutually approved by the Competent Security Authorities. The Receiving Party shall confirm the receipt of Classified Information at the levels TAJNO / SALAINEN or HEMLIG and above. The receipt of other Classified Information shall be confirmed on request.

2. Classified Information shall be transmitted electronically only by secure means agreed between the Competent Security Authorities.

## **Article 7**

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

1. Information classified at the VRLO TAJNO / ERITTÄIN SALAINEN or YTTERST HEMLIG level shall be translated or reproduced only in exceptional cases upon prior written consent of the Originating Party.

2. All copies of Classified Information shall be marked with the original classification marking. Such reproduced information shall be protected in the same way as the original information. The number of copies shall be limited to that required for official purposes.

3. Any translation of Classified Information shall be marked with the original classification marking and bear an additional note in the language of translation that the translation contains Classified Information of the Originating Party.

## **Article 8**

### **Destruction of Classified Information**

1. Classified Information shall be destroyed insofar as to prevent its reconstruction in whole or in part.

2. Classified information at the VRLO TAJNO / ERITTÄIN SALAINEN or YTTERST HEMLIG level shall not be destroyed. It shall be returned to the Originating Party.

3. The Originating Party may, by additional marking or subsequent written notice, expressly prohibit the destruction of Classified Information. If the destruction of Classified Information is prohibited, it shall be returned to the Originating Party.

4. In case of a crisis situation which makes it impossible to protect or return Classified Information generated or exchanged under this Agreement the Classified Information shall be destroyed immediately. The Receiving Party shall notify the National Security 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 of each Party.

2. Upon request the National Security 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 National Security Authority of the Receiving Party to issue the appropriate security clearance.

3. A Facility Security Clearance is not required for Classified Contracts at the OGRANIČENO / KÄYTTÖ RAJOITETTU or BEGRÄNSAD TILLGÅNG level.

4. Each Classified Contract or sub-contract shall include security provisions by which the Originating Party shall specify the Classified Information to be released to the Receiving Party, the Security Classification Level assigned to that information, and the Contractor's obligations to protect the Classified Information.

5. The Contractor's obligations to protect Classified Information shall include, at least, the following:

- a) to grant access to the Classified Information in accordance with the national laws and regulations and this Agreement;
- b) to transmit the Classified Information by the means specified in this Agreement;
- c) to communicate any changes that may arise in respect of the Classified Information;
- d) to use the Classified Information under the Classified Contract only for the purposes related to the subject of the contract;
- e) to adhere strictly to the provisions of this Agreement related to the procedures for handling Classified Information;
- f) to notify the Contractor's National Security Authority of any Security Breach related to the Classified Contract;
- g) to release the Classified Information related to the Classified Contract to any Third Party only upon prior written consent of the Originating Party.

6. Sub-contractors engaged in Classified Contracts shall, as appropriate, comply with the security provisions applied to the Contractors.

## **Article 10**

### **Visits**

1. Visits entailing access to Classified Information are subject to prior permission by the National Security Authority of the host Party. The permission shall be granted on the basis of a visit request by the National Security Authority of the visiting Party.

2. The request referred to in paragraph 1 of this Article shall contain:

- a) the visitor's name and surname, date and place of birth, and nationality;
- b) the passport number or another identification card number of the visitor;
- c) the position of the visitor and the name of the organization represented;
- d) the level of the Personnel Security Clearance of the visitor;
- e) the purpose, proposed working programme, including the highest level of Classified Information involved, and planned date of the visit;
- f) the names of the organizations and facilities requested to be visited;

- g) the number of visits and the period required;
- h) any other data, agreed upon by the National Security Authorities.

3. The request referred to in paragraph 1 of this Article shall be submitted at least 3 weeks in advance. In urgent cases the National Security Authorities may agree on a shorter period.

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

## **Article 11**

### **Security Breach**

1. In case of a Security Breach, the National Security Authority of the Party where the breach has occurred shall, without delay, inform the National Security Authority of the Originating Party about the breach and, in accordance with national laws and regulations, initiate appropriate proceedings in order to determine the circumstances of the Security Breach. The results of the proceedings shall be forwarded to the National Security Authority of the Originating Party.

2. When the Security Breach has occurred in a third state, the National Security Authority of the sending Party shall take the actions referred to in paragraph 1 of this Article without delay.

## **Article 12**

### **Expenses**

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

## **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 and shall not be referred to any international tribunal or Third Party for settlement.

## **Article 14**

### **Final Provisions**

1. This Agreement shall enter into force on the first day of the second month following the receipt of the last written notification by which the Parties have informed each other, through

diplomatic channels, that their internal legal requirements necessary for the entry into force of the Agreement have been fulfilled.

2. This Agreement may be amended by mutual written consent of the Parties. The 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 Zagreb on 11 February 2014 in two originals, each in the Croatian, Finnish 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 FINLAND**