

AGREEMENT

BETWEEN

THE GOVERNMENT OF THE REPUBLIC OF CROATIA

AND

THE GOVERNMENT OF THE REPUBLIC OF ESTONIA

ON MUTUAL PROTECTION OF CLASSIFIED INFORMATION

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

realizing 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 transmitted or generated in the course of the cooperation between 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 the form, which requires protection against security compromise and has been classified in accordance with national laws and regulations of the originating Party;

(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) “**Security Compromise**” means any form of disclosure, misuse, unauthorized alteration, damage or destruction of Classified Information, as well as any other action or inaction, resulting 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 that has created the Classified Information;

(6) “**Receiving Party**” means the Party 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 Authority**” means the National 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 contains or the execution of which requires access to Classified Information;

(11) “**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;

(12) “**Facility Security Clearance**” means the determination by the Competent Authority confirming in accordance with national laws and regulations that the legal entity or individual has the physical and organizational capability to meet 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

The Parties agree that the following Security Classification Levels are equivalent:

For the Republic of Croatia	Equivalent in English	For the Republic of Estonia
VRLO TAJNO	TOP SECRET	TÄIESTI SALAJANE
TAJNO	SECRET	SALAJANE
POVJERLJIVO	CONFIDENTIAL	KONFIDENTSIAALNE
OGRANIČENO	RESTRICTED	PIIRATUD

Article 4

National 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 Estonia:

- Security Department of the Ministry of Defence.

2. The Parties shall inform each other through diplomatic channels of changes of the National Security Authorities.

3. On request, the National Security Authorities shall inform each other of 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.

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, 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, 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. Classified Information shall only be made accessible to persons 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.

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

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

6. 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 the Security Classification Level.

7. 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.

8. 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.

9. 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 channels mutually approved by the National Security Authorities. The Receiving Party shall confirm the receipt of Classified Information in writing.

2. The security and police services of the Parties may directly exchange operative information in accordance with national laws and regulations.

Article 7

Reproduction and Translation of Classified Information

1. Information classified as TAJNO / SECRET / SALAJANE or above 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 placed under the same control as the original information. The number of copies shall be restricted to that required for official purposes.

3. 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 8

Destruction of Classified Information

1. Classified Information shall be destroyed insofar as to prevent its reconstruction in whole or in part.
2. Information classified as VRLO TAJNO / TOP SECRET / TÄIESTI SALAJANE 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 destruction of Classified Information. If destruction of Classified Information is prohibited, it shall be returned to the Originating Party.
4. In crisis situation in which it is impossible to protect or return Classified Information transmitted or generated under this Agreement, the Classified Information shall be destroyed immediately. The Receiving Party shall inform 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 the appropriate clearance, the National Security Authority of the Originating Party may request the National Security Authority of the Receiving Party to issue the appropriate clearance.
3. 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.
4. 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 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;
 - b) transmission of Classified Information by the means in accordance with this Agreement;
 - c) the procedures 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 National Security Authority of any Security Compromise related to the Classified Contract;
- g) release of Classified Information related to the Classified Contract to any Third Party only upon prior written consent of the Originating Party.

Article 10

Visits

1. Visits related to the execution or preparation of a Classified Contract requiring 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 include:
 - a) visitor's name, date and place of birth, citizenship;
 - 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;
 - e) purpose, proposed working program and planned date of the visit;
 - f) names of organizations and facilities to be visited;
 - g) number of visits and period required;
 - h) other data, if agreed upon by the National Security Authorities.
3. Each Party shall guarantee the protection of personal data of the visitors in accordance with its national laws and regulations.

Article 11

Security Compromise

1. In case of actual or suspected Security Compromise, the National Security Authority of the Party where it has occurred shall, without delay, inform the National Security Authority of the Originating Party and, in accordance with national laws and regulations, initiate appropriate proceedings, in order to determine the circumstances of the compromise. The results of the proceedings shall be forwarded to the National Security Authority of the Originating Party.
2. When the Security Compromise 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 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 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 paragraph 1 of this Article.
3. This Agreement is concluded for an indefinite period of time. Either Party may terminate this Agreement by giving the other Party notice in writing through diplomatic channels. In that case, this Agreement shall terminate six months from the date on which the other Party has received the termination 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 and, upon request, returned to the Originating Party.

Done at _____ on _____ in two originals, each in the Croatian, Estonian 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 Estonia**
