

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

The Government of the Republic of Croatia and the Government of Romania (hereinafter: the Parties),

Realizing that good cooperation may require exchange of classified information between the Parties, directly or through other legal entities,

Desiring to create a set of rules regulating the mutual protection of classified information applicable to any future co-operation agreements and contracts, which will be implemented between the Parties, or between legal entities of their states, containing or providing for access to classified information,

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 exchanged or created in the process of cooperation between the Parties or between legal entities of the states of the Parties.
2. This Agreement is applicable to any activity involving the exchange of Classified Information, conducted or to be conducted between the Parties or between legal entities of the states of the Parties.
3. This Agreement shall not affect the commitments of both Parties which stem from other international agreements by which they are bound and shall not be used against the interests, security and territorial integrity of other states.

## **ARTICLE 2 DEFINITIONS**

In this Agreement, the following definitions shall be used:

- (1) **Classified Information:** Any information, document or material, regardless of its physical form, to which a particular classification level has been assigned in accordance with the legislations of the states of the Parties and which shall be protected appropriately;
- (2) **Classification Level:** A category which, in accordance with the legislation of the state of the Party, determines certain restrictions of access to Classified Information, measures of protection and markings;
- (3) **Originating Party:** The Party, including any other legal entity of its state, which creates and releases Classified Information to the other Party;
- (4) **Recipient Party:** The Party, including any other legal entity of its state, which receives Classified Information from the other Party;
- (5) **Classified Contract:** A contract or sub-contract that contains or involves access to Classified Information;
- (6) **Personnel Security Certificate:** A document issued in accordance with the legislation of the state of the Party and stemming from a vetting procedure finalized with a positive decision, which enables a person to be granted access and permission to handle Classified Information of a certain classification level;

- (7) **Facility Security Certificate:** A document issued in accordance with the legislation of the state of the Party and stemming from a vetting procedure finalized with a positive decision, which is to enable a legal entity to carry out activities related to a Classified Contract;
- (8) **Competent Security Authority:** The institution listed in Article 3, empowered with authority at national level which, in accordance with the legislation of the state of the Party, ensures the unitary implementation of the protective measures for Classified Information;
- (9) **Need-to-know principle:** A principle by which access to Classified Information may be granted to an individual in order to be able to perform official duties and tasks;
- (10) **Compromise:** Any form of misuse, contrary to the legislation of the state of the Party, which results in damage or unauthorized access, alteration, disclosure or destruction of Classified Information, as well as any other action or inaction, resulting in loss of its confidentiality, integrity or availability.

**ARTICLE 3  
COMPETENT SECURITY AUTHORITIES**

- 1. The Competent Security Authorities responsible for the implementation of this Agreement are:  
 For the Republic of Croatia:  
 Office of the National Security Council  
  
 For Romania:  
 Government of Romania  
 National Registry Office for Classified Information.
- 2. The Parties shall inform each other through diplomatic channels of any relevant change regarding the Competent Security Authorities.

**ARTICLE 4  
CLASSIFICATION LEVELS**

- 1. The equivalence of national classification levels is as follows:

<b>For the Republic of Croatia</b>	<b>For Romania</b>
VRLO TAJNO	STRICT SECRET DE IMPORTANȚĂ DEOSEBITĂ
TAJNO	STRICT SECRET
POVJERLJIVO	SECRET
OGRANIČENO	SECRET DE SERVICIU

- 2. The Originating Party shall without delay notify the Recipient Party of any changes to the classification level of released Classified Information.
- 3. The Originating Party shall inform the Recipient Party of additional conditions of release or limitations on the use of released Classified Information.
- 4. The Recipient Party shall ensure that received Classified Information is marked with an equivalent national Classification Level in accordance with paragraph 1 of this Article.

5. The assignment of a Classification Level to jointly created Classified Information, its change and the declassification of this information shall be made upon common consent of the Parties.
6. The Parties shall notify each other of any changes to national classification levels.

## **ARTICLE 5 PROTECTION OF CLASSIFIED INFORMATION**

1. The Recipient Party shall provide to all received Classified Information the same protection as it is provided for the national Classified Information with the equivalent Classification Level, in accordance with Article 4 paragraph 1.
2. Nothing in this Agreement shall cause prejudice to the legislation of the state of the Party regarding public access to documents or access to information of public character, the protection of personal data or the protection of Classified Information.
3. Each Party shall ensure that appropriate measures are implemented for the protection of Classified Information processed, stored or transmitted in communication and information systems. Such measures shall ensure the confidentiality, integrity, availability and, where applicable, non-repudiation and authenticity of Classified Information, as well as an appropriate level of accountability and traceability of actions in relation to that information.

## **ARTICLE 6 DISCLOSURE AND USE OF CLASSIFIED INFORMATION**

1. Each Party shall ensure that Classified Information provided or exchanged under this Agreement is not:
  - a) downgraded or declassified without the prior written consent or at the request of the Originating Party;
  - b) used for purposes other than it was provided for and out of the limitations stated by the Originating Party;
  - c) disclosed to any third state, international organisation, individual or legal entity without the prior written consent of the Originating Party.
2. If any other agreement concluded between the Parties contains stricter regulations regarding the exchange or protection of Classified Information, these regulations shall apply.

## **ARTICLE 7 ACCESS TO CLASSIFIED INFORMATION**

1. Access to information classified POVJERLJIVO/SECRET and above and/or to locations and facilities where activities involving such information are performed is allowed, with the observance of the Need-to-know principle, only to individuals authorised and having a Personnel Security Certificate valid for the Classification Level of the information for which the access is required.

2. Access to information classified OGRANIČENO/SECRET DE SERVICIU shall be limited to those persons who have Need-to-know and provided they meet the requirements for access to such Classified Information in accordance with the legislation of the state of the Party.
3. Each Party shall ensure that all individuals granted access to Classified Information are informed of their responsibilities to protect such information in accordance with the appropriate security regulations.
4. On request, the Parties, through their Competent Security Authorities, shall confirm that a Personnel Security Certificate is granted to an individual before accessing Classified Information of the Originating Party.

## **ARTICLE 8 TRANSLATION AND REPRODUCTION OF CLASSIFIED INFORMATION**

1. All translations and reproductions of Classified Information shall be marked with the appropriate national classification level and shall be protected as the original Classified Information.
2. All translations and reproductions of Classified Information shall be made by persons having appropriate Personnel Security Certificates.
3. All translations of Classified Information shall contain a suitable annotation in the language of translation, indicating that they contain Classified Information of the Originating Party.
4. Classified Information marked VRLO TAJNO/STRICT SECRET DE IMPORTANTĂ DEOSEBITĂ shall be translated or reproduced only upon the prior written permission of the Originating Party.
5. All reproductions and translations of Classified Information shall be placed under the same protective measures as the original information. The number of copies shall be limited to that required for official purposes.

## **ARTICLE 9 DESTRUCTION OF CLASSIFIED INFORMATION**

1. Classified Information shall be destroyed in accordance with the legislation of the state of the Recipient Party, in such a manner as to eliminate its reconstruction in part or in whole.
2. Classified Information shall be destroyed only with the prior written consent of or at the request of the Originating Party.
3. VRLO TAJNO/STRICT SECRET DE IMPORTANTĂ DEOSEBITĂ information shall not be destroyed. It shall be returned to the Originating Party after it is no longer considered necessary by the Recipient Party or upon request of the Originating Party.
4. The Recipient Party shall inform in writing the Originating Party of the destruction of Classified Information.

5. In case of a situation that makes it impossible to protect and return Classified Information created or released according to this Agreement, the Classified Information shall be destroyed immediately. The Recipient Party shall notify in due time the Competent Security Authority of the Originating Party about the destruction of the Classified Information.

## **ARTICLE 10 TRANSFER OF CLASSIFIED INFORMATION**

1. Classified Information shall be transferred by diplomatic channels, military courier or other means agreed on by the Competent Security Authorities in accordance with the legislation of the state of the Party initiating the transfer. The Recipient Party shall acknowledge in writing the receipt of the Classified Information.
2. Classified Information shall be transferred electronically in cryptic form, by using the cryptographic methods and devices mutually accepted by the Competent Security Authorities in accordance with the legislation of the state of the Party.
3. If a large consignment containing Classified Information is to be transferred the Competent Security Authorities shall agree upon the means of transportation, the route and security measures for each such case.

## **ARTICLE 11 VISITS**

1. Visits entailing access to Classified Information on the territory of the state of the host Party are subject to prior written authorisation given by the Competent Security Authority of the host Party, or otherwise agreed upon between them, in accordance with the legislation of its state.
2. A request for visit shall be submitted to the Competent Security Authority of the host Party and shall include the following data that shall be used for the purpose of the visit only:
  - a) the visitor's name, date and place of birth, citizenship and identification card/passport number;
  - b) the visitor's position, with specification of the employer that the visitor represents;
  - c) specification of the project in which the visitor is participating;
  - d) confirmation of the visitor's Personnel Security Certificate, its validity and the Classification Level of the information up to which it may grant access;
  - e) the name, address, phone/fax number, e-mail and point of contact of the facility to be visited;
  - f) the purpose of the visit, including the highest Classification Level of Classified Information involved;
  - g) the date and duration of the visit. For recurring visits, the total period covered by the visits shall be stated;
  - h) other data, if agreed upon by the Competent Security Authorities;
  - i) date, signature and stamp of the Competent Security Authority of the requesting Party.

3. A request for visit shall be submitted at least 20 days prior to the visit, unless otherwise mutually approved by the Competent Security Authorities.
4. The Competent Security Authority of the Party receiving the request for visit shall inform, in due time, the Competent Security Authority of the requesting Party about the decision.
5. Once the visit has been approved, the Competent Security Authority of the host Party shall provide a copy of the request for visit to the security officer of the facility to be visited.
6. Visitors shall comply with the security regulations and instructions of the host Party.
7. The Competent Security Authorities may agree on a list of visitors entitled to recurring visits. The list shall be valid for an initial period not exceeding 12 months and may be extended for a further period of time not exceeding 12 months. A request for recurring visits shall be submitted in accordance with paragraph 3 of this Article. Once the list has been approved, visits may be arranged directly between the facilities involved.
8. The host Party shall guarantee the protection of personal data of the visitors in accordance to the legislation of its state.

## **ARTICLE 12 CLASSIFIED CONTRACTS**

1. In the event that a Party or a legal entity of its state intends to conclude a Classified Contract to be performed within the territory of the state of the other Party, then the Party on whose territory the performance is taking place will assume responsibility for the protection of Classified Information related to the contract in accordance with the legislation of its state and the provisions of this Agreement.
2. On request, the Competent Security Authorities shall confirm whether the proposed contractors as well as the individuals participating in pre-contractual negotiations or in the performance of Classified Contracts have been issued appropriate Facility Security Certificates and Personnel Security Certificates, before accessing Classified Information of the Originating Party.
3. Every Classified Contract concluded between contractors, under the provisions of this Agreement, shall include an appropriate security annex identifying at least the following aspects:
  - a) a listing of Classified Information related to the Classified Contract and its Classification Levels;
  - b) procedure for the communication of changes in the Classification Levels of the exchanged information;
  - c) communication channels and means for electromagnetic transmission;
  - d) procedure for the transportation of Classified Information;
  - e) an obligation to notify any actual or suspected Compromise.
4. A copy of the security annex of any Classified Contract shall be forwarded to the Competent Security Authority of the Party on whose territory the Classified Contract is to be performed, in order to allow adequate security supervision and control.

5. Classified Contracts entailing access to OGRANIČENO/SECRET DE SERVICIU information shall contain an appropriate clause identifying the minimum measures to be implemented for the protection of such Classified Information.
6. Any sub-contractor must fulfil the same security obligations as the contractor.
7. The Competent Security Authorities may agree on mutual visits in order to analyze the efficiency of the measures adopted by a contractor or a sub-contractor for the protection of Classified Information involved in a Classified Contract.
8. The Parties shall ensure protection of copyrights, industrial property rights – including patents, trade secrets and any other rights connected with the Classified Information exchanged between their states, according to the legislations of their states.
9. Further detailed procedures related to Classified Contracts may be agreed upon between the Competent Security Authorities of the Parties.

### **ARTICLE 13 SECURITY CO-OPERATION**

1. In order to achieve and maintain comparable standards of security, the Competent Security Authorities shall, on request, provide each other with information about their national security standards, procedures and practices for the protection of Classified Information. To this end, the Competent Security Authorities may conduct mutual visits.
2. If the need arise, the Competent Security Authorities may conclude security arrangements on specific technical aspects concerning the implementation of this Agreement.
3. The Competent Security Authorities shall inform each other of specific security risks that may endanger released Classified Information, as applicable.
4. On request, the Competent Security Authorities of the Parties, taking into account the legislations of their states, shall assist each other in the procedure of granting the Personnel Security Certificates and the Facility Security Certificates of their nationals living or facilities located on the territory of the state of the other Party.
5. The Competent Security Authorities shall inform each other about any modifications regarding the Personnel Security Certificates and Facility Security Certificates, which are connected to the cooperation under this Agreement.
6. The Parties shall mutually recognise their respective Personnel Security Certificates and Facility Security Certificates, issued for the citizens and legal entities of their states, in accordance with the legislations of their states, as regards the access to Classified Information exchanged under this Agreement.
7. The security and intelligence services of the states of the Parties may cooperate and directly exchange operative and/or intelligence information in accordance with the legislations of their states.

## **ARTICLE 14 COMPROMISE**

1. The Parties shall take all appropriate measures, in accordance with the legislations of their states, to determine the circumstances where it is known or where there are reasonable grounds for suspecting that Classified Information has been compromised.
2. In case of a Compromise involving Classified Information originated by and received from the other Party, the Competent Security Authority in whose state the Compromise occurred shall inform the Competent Security Authority of the Originating Party as soon as possible and ensure the implementation of appropriate measures in accordance with the legislation of its state. The Parties shall, if required, cooperate during the above referred proceedings.
3. In case the Compromise occurs on the territory of a third state, the Competent Security Authority of the dispatching Party shall take the actions referred to in paragraph 2 of this Article.
4. In any case, the Competent Security Authority of the Recipient Party shall inform the Competent Security Authority of the Originating Party in writing about the circumstances of the Compromise, the extent of the damage, the measures taken for its mitigation and the outcome of the proceedings referred to in paragraph 2 of this Article. Such notification shall contain enough details so that the Originating Party may fully assess the consequences.

## **ARTICLE 15 SETTLEMENT OF DISPUTES**

Any dispute between the Parties relating to the interpretation or application of this Agreement shall be settled through consultations between the Parties only.

## **ARTICLE 16 EXPENSES**

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

## **ARTICLE 17 FINAL PROVISIONS**

1. This Agreement is concluded for an indefinite period of time. It is subject to approval in accordance with the legal procedures of the state of each Party and shall enter into force on the first day of the second month following the date of receipt of the last written notification by which the Parties have informed each other, through diplomatic channels, that their internal legal requirements for the entry into force of this Agreement have been met.

2. This Agreement may be amended at any time by mutual written consent of the Parties. Such amendments shall enter into force in accordance with the provisions of paragraph 1 of this Article.
3. Each Party may terminate this Agreement at any time by written notification to the other Party through diplomatic channels. In this case, the Agreement shall terminate after six (6) months from the date of receipt of the termination notification by the other Party.
4. Notwithstanding the termination of this Agreement, all Classified Information released under this Agreement shall continue to be protected in accordance with the provisions set out herein until the Originating Party dispenses the Recipient Party from this obligation.
5. The Parties shall promptly notify each other of any amendments to legislation of their states that affect the protection of Classified Information released under this Agreement. In the event of such amendments, the Parties shall consult to consider possible amendments to this Agreement. In the meantime, Classified Information shall continue to be protected as described herein, unless otherwise requested by the Originating Party in writing.

In witness whereof, the undersigned, duly authorised to this effect by their respective Governments, have signed this Agreement.

Done at Zagreb on 12 June 2017 in two originals, each in the Croatian, Romanian and English languages, all texts being equally authentic. In case of divergences of interpretation, the English text shall prevail.

**FOR THE GOVERNMENT OF  
THE REPUBLIC OF CROATIA**

**FOR THE GOVERNMENT OF  
ROMANIA**