

**Agreement
between
the Government of the Republic of Croatia
and
the Government of the Slovak Republic
on Mutual Protection of Classified Information**

The Government of the Republic of Croatia
and
the Government of the Slovak Republic

(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, economical, legal, scientific and technological or any other cooperation, as well as classified information arisen in the process of such cooperation,

Intending to ensure the mutual protection of all Classified Information, which has been classified in the state of the one Party and transferred to the state of the other Party,

Desiring to create a set of rules on the mutual protection of Classified Information exchanged between the Parties,

Considering the mutual interests in the protection of Classified Information, in accordance with the legislation of the states of the both 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 states of the Parties.

**Article 2
Definitions**

For the purposes of this Agreement:

- a) “**Classified Information**” means any information or material, irrespective of its form or nature, which requires protection against unauthorized manipulation and has been classified in accordance with the national legislation of the states of the Parties;
- b) “**Originating Party**” means the state of the Party which transmits Classified Information to the state of the other Party;
- c) “**Receiving Party**” means the state of the Party which Classified Information is transmitted to by the state of the other Party;
- d) “**Competent Security Authority**” means the national security body responsible for the implementation and supervision of this Agreement;
- e) “**Contractor**” means an individual or a legal entity possessing the legal capacity to conclude Classified Contracts;
- f) “**Classified Contract**” means an agreement between two or more Contractors, which contains or involves Classified Information;

- g) **“Personnel Security Clearance”** means the determination by the Competent Security Authority confirming, in accordance with the respective national legislation, that the individual is eligible to have access to Classified Information;
- h) **“Facility Security Clearance”** means the determination by the Competent Security Authority confirming, that the legal entity has the physical and organizational capability to use and store Classified Information in accordance with the respective national legislation;
- i) **“Third Party”** means any state, organization, legal entity or individual, which is not a party to this Agreement;
- j) **“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.

Article 3 Security Classification Levels

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

For the Republic of Croatia	For the Slovak Republic	Equivalent in English
VRLO TAJNO	PRÍSNE TAJNÉ	TOP SECRET
TAJNO	TAJNÉ	SECRET
POVJERLJIVO	DÔVERNÉ	CONFIDENTIAL
OGRANIČENO	VYHRADENÉ	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 Slovak Republic:
National Security Authority.
2. The states of the Parties shall inform each other through diplomatic channels of any modification of contact data of the Competent Security Authorities.
3. On request, the Competent Security Authorities shall inform each other of respective national legislation on 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 legislation, the states of 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 assigned to such Classified Information as is provided for the national Classified Information of the equivalent security classification level in accordance with the Article 3.
2. The Originating Party shall inform the Receiving Party in writing about any change of the security classification level of the transmitted Classified Information.

3. Access to Classified Information shall be limited to persons on a Need-to-know basis who are authorized in accordance with the national legislation to have access to Classified Information of the equivalent security classification level.
4. Within the scope of this Agreement, state of each Party shall recognize the Personnel and Facility Security Clearances granted in accordance with the national legislation of the state of the other Party. The security clearances shall be equivalent in accordance with Article 3.
5. The Competent Security Authorities shall, in accordance with the national legislation, assist each other upon request at carrying out vetting procedures necessary for the application of this Agreement.
6. Within the scope of this Agreement, the Competent Security Authorities 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. The Receiving Party shall:
 - a) submit Classified Information to any Third Party only upon prior written consent of the Originating Party;
 - b) mark the received Classified Information in accordance with the Article 3;
 - c) 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 channels unless otherwise approved on by the Competent Security Authorities. 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 approved on by the Competent Security Authorities.

Article 7 Reproduction and Translation of Classified Information

1. Classified Information marked SECRET or above shall be translated or reproduced only upon prior written consent of the Originating Party.
2. Translations and reproductions of Classified Information shall be made in accordance with the following procedures:
 - a) the individuals shall hold the appropriate Personnel Security Clearance in accordance with their national legislation;
 - b) the translations and the reproductions shall be marked and protected as the original Classified Information;
 - c) the translations and the number of copies shall be limited to that required for official purposes;
 - d) the translations shall bear an appropriate note in the language of the translation indicating that it contains Classified Information received from the Originating Party.

Article 8
Destruction of Classified Information

1. Classified Information shall be destroyed so as to prevent its partial or total reconstruction.
2. Classified Information marked TOP SECRET shall not be destroyed. It shall be returned to Competent Security Authority of the Originating Party.
3. Classified Information marked up to SECRET shall be destroyed in accordance with the national legislation.
4. A report on destruction of Classified Information shall be made and its translation in English shall be delivered to the Competent Security Authority of the Originating Party.

Article 9
Classified Contracts

1. State of one Party, wishing to place a Classified Contract with a Contractor of the state of the other Party, or wishing to authorize one of its own Contractors to place a Classified Contract in the territory of the state of the other Party within a classified project shall obtain, through its Competent Security Authority, prior written assurance from the Competent Security Authority of the state of the other Party that the proposed Contractor holds Facility Security Clearance of the appropriate security classification level.
2. Each Classified Contract concluded in accordance with this Agreement shall include:
 - a) commitment of the Contractor to ensure that its premises have necessary conditions for handling and storing Classified Information of appropriate security classification level;
 - b) commitment of the Contractor to ensure that persons who perform duties requiring access to Classified Information hold the appropriate level of Personnel Security Clearance;
 - c) commitment of the Contractor to ensure that all persons with access to Classified Information are informed of their responsibility towards the protection of Classified Information in accordance with the national legislation;
 - d) commitment of the Contractor to perform periodical security inspections of its premises;
 - e) list of Classified Information and list of areas in which Classified Information can arise;
 - f) procedure for communication of changes in the security classification level of Classified Information;
 - g) communication means and electronic means for transmission;
 - h) procedure for the transportation of Classified Information;
 - i) appropriate authorized individuals or legal entities responsible for the co-ordination of the safeguarding of Classified Information related to the Classified Contract;
 - j) commitment of the Contractor to notify any actual or suspected loss, leak or compromise of the Classified Information;
 - k) commitment of the Contractor to forward a copy of the Classified Contract to its own Competent Security Authority;
 - l) commitment of the subcontractor to fulfill the same security obligations as the Contractor.

3. As soon as pre-contractual negotiations begin between a potential Contractor in the territory of one state of the Parties and another possible Contractor located in the state of the other Party's territory, aiming at the signing of Classified Contracts, the Competent Security Authority shall inform the state of the other Party of the security classification level given to the Classified Information related to those pre-contractual negotiations.
4. Copy of each Classified Contract shall be forwarded to the Competent Security Authority of the state of the Party where the work is to be performed, to allow adequate security supervision and control.
5. Representatives of the Competent Security 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. Notice of the visit shall be provided, at least, twenty days in advance.

Article 10 **Visits**

1. Visits involving access to Classified Information by nationals from the state of one Party to the state of the other Party are subject to prior written approval given by the Competent Security Authority of the host state.
2. Visits involving access to Classified Information shall be allowed by the state of one Party to visitors from the state of the other Party only if they have been:
 - a) granted appropriate Personnel Security Clearance by the Competent Security Authority of the sending state;
 - b) authorized to receive or to have access to Classified Information in accordance with their national legislation.
3. Visits involving access to Classified Information by nationals from a third state shall only be authorized by a common agreement between the states of the Parties.
4. The Competent Security Authority of the sending state shall notify the Competent Security Authority of the host state of the planned visit through a request for visit, which has to be received at least thirty days before taking place.
5. In urgent cases, the request for visit shall be transmitted at least seven days before.
6. The request for visit shall include:
 - a) visitor's name and surname, place and date of birth, nationality, passport or identification document number;
 - b) name of the legal entity the visitor represents or to which the visitor belongs;
 - c) name and address of the legal entity to be visited;
 - d) confirmation of the visitor's Personnel Security Clearance and its validity;
 - 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) the date, signature and stamping of the official seal of the Competent Security Authority.
7. Once the visit has been approved the Competent Security Authority of the host state shall provide a copy of the request for visit to the security officers of the legal entity to be visited.
8. The validity of visit approval shall not exceed one year.

9. The states 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.

Article 11 Breach of Security

1. In case of breach of security in accordance with the national legislation that results in an actual or suspected compromise of Classified Information originated by or received from the state of the other Party, the Competent Security Authority of the state of the Party where the breach or compromise has arisen shall inform the Competent Security Authority of the state of the other Party, as soon as possible, and initiate the appropriate investigation.
2. If a breach of security arises in a state other than states of the Parties, the Competent Security Authority of the dispatching state shall take the actions prescribed in Paragraph 1.
3. The state of the other Party shall, upon request, co-operate in the investigation in accordance with Paragraph 1.
4. The state of the other 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 application and supervision of this Agreement.

Article 13 Settlement of Disputes

Any dispute regarding the interpretation or application of this Agreement shall be settled by negotiations between the Competent Security Authorities.

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 the 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.
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 the 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 Zagreb on 6 October 2009 in two originals, each in the Croatian, Slovak 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
SLOVAK REPUBLIC**