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

The Government of the Republic of Croatia and the Government of the Italian Republic (hereinafter referred to as "the Parties"),

Recognising the important role of their mutual co-operation for the stabilisation of peace, international security and mutual confidence,

Recognising the interest and the common necessity to ensure the protection of any Classified Information in the political, security, military, economic and any other field exchanged between the Parties and their public and private entities, in accordance with the laws and regulations of the Parties,

Recognising the need to establish common security regulations for the safeguarding of information, also in relation to the possibility of implementing technical cooperation agreements and developing contractual activities,

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

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

Have agreed as follows:

Article 1
Objective and Applicability

The objective of this Agreement is to ensure protection of Classified Information and to establish common procedures and rules for the protection of any Classified Information exchanged between the Parties and between the public and private entities of the Parties concerning international affairs, national security and defence, as well as industrial activities and operations.

Article 2
Definitions

For the purposes of this Agreement:

1. "**Classified Information**" means any information, record, activity, document, material, including objects and facilities, that a security classification level has been assigned to in accordance with the national laws and regulations;
2. "**Need-to-know**" means the principle upon which access to Classified Information is authorized only to individuals in relation to their need to perform their official functions and duties;

3. "**Breach of Security"** means the consequence of actions or omissions contrary to a provision concerning the protection of Classified Information that may result in a loss of confidentiality, integrity or availability of such information;
4. "**Security classification level**" means the 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, decided on the basis of the extent of the damage caused by an unauthorized access;
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 security 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. "**Contractors and Subcontractors**" means individuals or legal entities possessing the legal capacity to conclude contracts;
10. "**Classified Contract**" means an agreement between two or more Contractors, that will require access to or generation of 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 the respective level of 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 certified to handle and manage Classified Information to the respective level of classification;
13. "**Third Party**" means any State, organization and legal entity 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 prescribed by the national laws and regulations of the respective Party:

For the Republic of Croatia	For the Italian Republic	English translation
VRLO TAJNO	SEGRETISSIMO	TOP SECRET
TAJNO	SEGRETO	SECRET
POVJERLJIVO	RISERVATISSIMO	CONFIDENTIAL
OGRANIČENO	RISERVATO	RESTRICTED

Article 4
Competent Security Authorities

1. The Competent Security Authorities of the Parties are:

   For the Republic of Croatia:
   Ured Vijeća za nacionalnu sigurnost;

   For the Italian Republic:
   Dipartimento delle Informazioni per la Sicurezza (DIS)
   Ufficio Centrale per la Segretezza (UCSe).

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, as well as on any subsequent possible amendment to the national laws and regulations which govern the protection of Classified Information and any changes concerning the names and addresses of the Competent Security Authorities.

3. In order to ensure close co-operation in the implementation of this Agreement, the Competent Security Authorities may hold consultations.

4. The Parties shall mutually recognize the Facility and Personnel Security Clearance Certificates, released in accordance with the national laws and regulations.

5. The Competent Security Authorities shall ensure a strict and binding adherence to this Agreement by any public and private entity of the Parties, in accordance with national laws and regulations.

Article 5
Principles for the Mutual Protection of 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 or generated under this Agreement. Each Party shall ensure that any Classified Information of the other Party is assigned the same level of protection required by national laws and regulations for its Classified Information.

2. The Party cannot release to a Third Party any Classified Information of the other Party, nor downgrade or declassify the security classification level of Classified Information of the other Party, without the prior written consent of the Originating Party.

3. Both Parties are committed not to appeal to this Agreement to obtain any Classified Information which the other Party has obtained by a Third Party.

4. Access to Classified Information shall be granted on the basis of the need-to-know principle. Personnel Security Clearance Certificate and Facility Security Clearance Certificate shall be issued in accordance with the national laws and regulations of the Parties.

5. 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.

6. Principles for the mutual protection of Classified Information agreed between the Parties shall be applied in all other agreements and arrangements entailing the exchange of Classified Information between the Parties.

Article 6
Transmission of Classified Information

1. Information classified up to “TAJNO/SEGRETO/SECRET” level 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 from “POVJERLJIVO/RISERVATISSIMO/CONFIDENTIAL” level and above. Classified Information “VRLO TAJNO/SEGRETISSIMO/TOP SECRET” shall be sent only through certified military or diplomatic channels. In case of emergency, the Parties may arrange, on a case by case evaluation, different modalities of transmission of Classified Information.

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.

Article 7
Personnel Security Clearance Certificate

1. If an individual needs access to information classified as “POVJERLJIVO/RISERVATISSIMO/ CONFIDENTIAL” or above, to perform his/her official functions and duties, he/she shall hold an appropriate Personnel Security Clearance Certificate and need to be briefed accordingly. The Parties shall grant a Personnel Security Clearance Certificate, in compliance with their national laws and regulations.

2. The Competent Security Authorities shall assist each other, on request, during the vetting procedure for the release of Personnel Security Clearance Certificate.

3. The Competent Security Authorities shall also ensure mutual cooperation for possible requests for information on citizens of the other Party who lived or stayed in its territory.

Article 8
Marking of Classified Information

1. The Receiving Party shall mark the received Classified Information in accordance with the national laws and regulations and with the equivalent security classification level as defined in Article 3 of this Agreement.

2. Copies and translations of the received Classified Information shall be marked and handled in the same manner as the originals.

Article 9
Reproduction and Translation of Classified Information

1. Information classified as “VRLO TAJNO/SEGRETISSIMO/TOP SECRET” shall be translated or reproduced only in exceptional cases upon prior written consent 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 from “POVJERLJIVO/RISERVATISSIMO/ CONFIDENTIAL” level and above shall be made by security cleared individuals.

4. The translation of Classified Information 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 10
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 “VRLO TAJNO/SEGRETISSIMO/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 an emergency, 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 only about the destruction of information classified as “VRLO TAJNO/SEGRETISSIMO/TOP SECRET”.

Article 11
Classified Contracts

1. Contractors and Subcontractors which participate in negotiation and performing of classified contracts shall hold an appropriate Facility Security Clearance Certificate to the level required for the contract, to ensure the protection of Classified Information.

2. In the event that a public or private entity of one Party, duly cleared, awarded a contract to be performed within the national borders of the other Party, and such contract includes the exchange of Classified Information, the Party where the contract is to be performed, shall take appropriate security measures for the protection of Classified Information, in accordance with the national laws and regulations.

3. 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 confirm that a proposed Contractor has been granted an appropriate national Facility Security Clearance Certificate.

4. 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.

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

   a) release of Classified Information exclusively to persons who have been previously granted 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.

6. The measures required for the protection of Classified Information, as well as the procedure for assessment of any 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.

7. Classified Contracts of security classification level "OGRANIČENO/RISERVATO/ 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 12
Visits

1. Visits carried out by citizens of one Party to facilities of the other Party, who need access to Classified Information, shall be submitted to prior written authorization by the Competent Security Authority of the Party where the visit takes place.

2. Request for visit shall be forwarded at least 20 days in advance of the scheduled date. In case of visits of utmost importance and urgency and not previously scheduled, the request for visit shall be forwarded al least 5 days before the visit takes place.

3. Personnel of one of the Parties, making an official request for visit to the other Party, pursuant to this Agreement shall:

a) be authorized to receive or access to Classified Information according to the need-to-know principle, and

b) hold a Personnel Security Clearance Certificate, at least equal to the classification level of the information which needs to be accessed to.

4. The request for visit referred to in paragraph 2 of this Article shall include:

a) visitor's name and surname, date and place of birth, citizenship;

b) passport number or identification card number of the visitor;

c) position of the visitor and name of the organisation represented;

d) appropriate security clearance assurance on the basis of the Personnel Security Clearance Certificate of the visitor, if necessary;

e) indication of the security classification level of the information that needs to be accessed to;

f) indication of the point of contact at the public or private entity to be visited, including name and surname, e-mail address and telephone number;

g) purpose and planned date of the visit;

h) names of organisations and facilities to be visited;

i) number of visits and period required;

j) other data, if agreed upon by the Competent Security Authorities.

5. The Competent Security Authority of the host Party notifies the Competent Security Authority of the other Party, through the channels agreed, about its decision, with sufficient advance in respect of the scheduled date for visit.

6. Visits of personnel of the public or private entity of one of the Parties up to the level "OGRANIČENO/RISERVATO/RESTRICTED" shall be agreed directly with the public or private entity of the other Party. The hosting public or private entity shall notify its Competent Security Authority about the visit.

7. In case of projects or contracts which require recurring visits classified as "POVJERLJIVO/RISERVATISSIMO/CONFIDENTIAL" and above, the Competent Security Authorities of the Parties shall notify each other by sending a list of authorized personnel. Such list can not be valid more than 12 months.

8. 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.

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

Article 13
Breach 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 as well as the following measures adopted 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, if possible, shall take the actions referred to in paragraph 1 of this Article without delay.

Article 14
Expenses

1. The implementation of this Agreement does not include any cost.

2. In the event of costs incurred by one Party, these shall not be supported by the other Party.

Article 15
Settlement of Disputes

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

2. Meanwhile, the Parties shall continue to fulfil the provisions set forth in this Agreement.

Article 16
Final Provisions

1. This Agreement shall enter into force on 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 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. Each of the Parties 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 after the date on which the other Party has received the denunciation notice.

4. In case of termination of this Agreement, all Classified Information transmitted pursuant to this Agreement shall continue to be protected in accordance with the provisions set forth herein.

Done at Zagreb on 9 July 2019 in two originals, each in the Croatian, Italian 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 ITALIAN REPUBLIC