Agreement

between

the Government of the Republic of Croatia

and

the Government of the Federal Republic of Germany

on the

Exchange and Mutual Protection of Classified Information

The Government of the Republic of Croatia
and
the Government of the Federal Republic of Germany,
hereinafter referred to as “the Contracting Parties”,

Intending to ensure the protection of classified information that is exchanged between the competent authorities of the Republic of Croatia and of the Federal Republic of Germany as well as with contractors or between contractors of the two Contracting Parties,

Desirous of agreeing on a legal framework for the exchange and mutual protection of classified information that shall apply to all instruments on cooperation to be concluded between the Contracting Parties and to contracts involving an exchange of classified information,

Have agreed as follows:

Article 1
Definitions

(1) For the purposes of this Agreement

1. “classified information” is

a) in the Republic of Croatia
any information, regardless of its form, which requires protection and has been classified in accordance with national laws and regulations or released as such by another state, international organization or institution that the Republic of Croatia cooperates with;

b) in the Federal Republic of Germany
facts, items or intelligence which, regardless of how they are presented, are to be kept secret in the public interest. They shall be classified by, or at the instance of, an official agency in accordance with their need for protection;

2. a "classified contract" is a contract between an authority or an enterprise from the state of one Contracting Party (contract owner) and an enterprise from the state of the other Contracting Party (contractor); under such contract, classified information from the state of the contract owner is to be released to the contractor or is to be generated by the contractor or is to be made accessible to members of the contractor's staff who are to perform tasks in facilities of the contract owner.

(2) The classification levels are defined as follows:

1. In the Republic of Croatia, classified information is

a) VRLO TAJNO if its unauthorised disclosure and knowledge of it by unauthorised persons would result in exceptionally grave damage to national security and vital interests of the Republic of Croatia,

b) TAJNO if its unauthorised disclosure and knowledge of it by unauthorised persons would result in grave damage to national security and vital interests of the Republic of Croatia,

c) POVJERLJIVO if its unauthorised disclosure and knowledge of it by unauthorised persons would be damaging to national security and vital interests of the Republic of Croatia,

d) OGRANIČENO if its unauthorised disclosure and knowledge of it by unauthorised persons would be damaging to the functioning of state authorities.

2. In the Federal Republic of Germany, classified information is

a) STRENG GEHEIM if knowledge of it by unauthorised persons may pose a threat to the existence or vital interests of the Federal Republic of Germany or one of its *Länder* (federal states),

b) GEHEIM if knowledge of it by unauthorised persons may pose a threat to the security of the Federal Republic of Germany or one of its *Länder* (federal states), or may cause severe damage to their interests,

c) VS-VERTRAULICH if knowledge of it by unauthorised persons may be damaging to the interests of the Federal Republic of Germany or one of its *Länder* (federal states),

d) VS-NUR FÜR DEN DIENSTGEBRAUCH if knowledge of it by unauthorised persons may be disadvantageous to the interests of the Federal Republic of Germany or one of its *Länder* (federal states).

Article 2

Classification Levels

The Contracting Parties stipulate that the following classification levels are equivalent:

Republic of Croatia	Federal Republic of Germany
VRLO TAJNO	STRENG GEHEIM
TAJNO	GEHEIM
POVJERLJIVO	VS-VERTRAULICH
OGRANIČENO	VS-NUR FÜR DEN DIENSTGEBRAUCH

Article 3

Marking

(1) Transmitted classified information shall be marked additionally with the equivalent national classification level as provided under Article 2 by, or at the instance of, the competent security authority of the recipient.

(2) Classified information which is generated in the state of the receiving Contracting Party in connection with classified contracts as well as copies, excerpts and translations made in the state of the receiving Contracting Party shall also be marked accordingly.

(3) The translation shall bear an appropriate note in the language into which it is translated that the translation contains classified information of the originating Contracting Party.

(4) The decision on the amendment or revocation of classification levels shall be taken only by the competent security authorities of the originating Contracting Party. The competent security authority of the originating Contracting Party shall inform the competent security authority of the receiving Contracting Party immediately of the amendment or revocation of any classification level. The competent security authority of the receiving Contracting Party shall implement this amendment or revocation accordingly.

Article 4

Measures at the National Level

(1) Within the scope of their respective national laws and regulations, the Contracting Parties shall take all appropriate measures to guarantee the protection of classified information generated, exchanged or handled under the terms of this Agreement. They shall afford such classified information a degree of protection comparable to that required by the receiving Contracting Party for its own classified information of the equivalent classification level.

(2) The classified information shall be used solely for the designated purpose. The receiving Contracting Party shall use or grant access, or shall permit the use or granting of access of any classified information only for the purposes and within any limitations stated by or on behalf of the originating Contracting Party. The originating Contracting Party must have given its written consent to any alternative arrangement prior to disclosure of the classified information.

(3) Access to classified information may be granted only to persons having a need-to-know on account of their duties and – except in the case of classified information at the OGRANIČENO / VS-NUR FÜR DEN DIENSTGEBRAUCH level – having been security-cleared or by virtue of their function being entitled to have access to classified information of the equivalent classification level. A security clearance shall be granted only after completion of a security screening under standards comparable to those applied for access to national classified information of the equivalent classification level.

(4) Access to classified information at the POVJERLJIVO / VS-VERTRAULICH level or higher by a national of the state of one Contracting Party shall be granted without the prior authorisation of the originating Contracting Party.

(5) Personnel Security Clearances for nationals of the state of a Contracting Party who reside and require access to classified information in their own state shall be conducted by their competent security authorities.

(6) Articles 6 and 7 of this Agreement shall not apply to classified information at the OGRANIČENO / VS-NUR FÜR DEN DIENSTGEBRAUCH level.

(7) The Contracting Parties shall, each within their state, ensure that the necessary security inspections are carried out and that this Agreement is complied with.

Article 5

Destruction of Classified Information

(1) Classified information shall be destroyed in a way which eliminates the possibility of its partial or total reconstruction.

(2) Classified information at the VRLO TAJNO / STRENG GEHEIM level shall not be destroyed. It shall be returned to the originating Contracting Party upon request or if the designated purpose has ceased to exist.

(3) Classified information at the TAJNO / GEHEIM or POVJERLJIVO / VS-VERTRAULICH level may be destroyed subject to the approval of the originating Contracting Party in writing.

(4) Classified information at the OGRANIČENO / VS-NUR FÜR DEN DIENSTGEBRAUCH level may be destroyed by the receiving Contracting Party if the designated purpose has ceased to exist.

(5) In a crisis situation in which it is impossible to protect or return classified information exchanged or generated under this Agreement, the classified information shall be destroyed immediately. The receiving Contracting Party shall inform the competent security authority of the originating Contracting Party about this destruction as soon as possible.

Article 6

Award of Classified Contracts

(1) Prior to the award of a classified contract, the contract owner shall, through its competent security authority, obtain a Facility Security Clearance from the competent security authority of the contractor in order to obtain assurance as to whether the prospective contractor is subject to security oversight by the competent security authority of its state and whether such contractor has taken the security precautions required for discharging the performance of the classified contract. Where a contractor is not yet subject to security oversight, an application may be made to that end.

(2) A Facility Security Clearance shall also be obtained if a potential contractor has been requested to submit a bid and if classified information of the POVJERLJIVO / VS-VERTRAULICH level or higher will have to be released prior to the award of a classified contract under the bid procedure.

(3) In the cases referred to in paragraphs (1) and (2) above, the following procedure shall be applied:

1. Requests for the issuance of a Facility Security Clearance for contractors from the state of the other Contracting Party shall contain information on the project as well as the nature, the scope and the classification level of the classified information expected to be released to the contractor or to be generated by it.

2. In addition to the full name of the contractor, its postal address, the name of its security official, his telephone and fax number and his e-mail address, Facility Security Clearances must include information in particular on the extent to which, and the classification level up to which security measures have been taken by the respective contractor on the basis of its national laws and regulations.

3. The competent security authorities of the Contracting Parties shall inform each other of any changes in the facts on the basis of which Facility Security Clearances have been issued.

4. The exchange of such information between the competent security authorities of the Contracting Parties shall be effected either in the national language of the authority to be informed or in English.

5. Facility Security Clearances and requests addressed to the respective competent security authorities of the Contracting Parties for the issuance of Facility Security Clearances shall be transmitted in writing.

Article 7
Performance of Classified Contracts

(1) Classified contracts must contain a security requirements clause under which the contractor is under an obligation to make the arrangements required for the protection of classified information pursuant to the national laws and regulations of its state.

(2) In addition, the security requirements clause shall contain the following provisions:

1. the definition of the term “classified information” and of the equivalent classification levels of the states of the two Contracting Parties in accordance with the provisions of this Agreement;

2. the requirement that classified information shall only be disclosed to a third party, or that such disclosure to a third party shall only be permitted, if this has been approved by the originating Contracting Party in writing;

3. the requirement that the contractor shall grant access to classified information only to a person who has a need-to-know and has been charged with, or contributes to, the performance of the classified contract and – except in the case of classified information at the OGRANIČENO / VS-NUR FÜR DEN DIENSTGEBRAUCH level – has been security-cleared to the appropriate classification level in advance;

4. the names of the respective competent authorities of the Contracting Parties in charge of authorising the release of classified information in connection with the award of classified contracts or entitled to coordinate the safeguarding of such classified information;

5. the channels to be used for the transfer of classified information between the competent authorities and contractors involved;

6. the procedures and mechanisms for communicating changes that may arise in respect of classified information either because of the amendment or revocation of its classification levels;

7. the procedures for the approval of visits to facilities, or access to classified information, by personnel of the contractors;

8. the procedures for transmitting classified information to contractors handling such classified information; and

9. the requirement that the contractor shall immediately notify its competent authority of any actual or suspected loss, leak or unauthorised disclosure of the classified information covered by the classified contract.

(3) The competent security authority of the contract owner shall provide the contractor with a separate list (classification guide) of all documentary records requiring security classification, shall determine the required classification level and shall arrange for this

classification guide to be enclosed as an appendix to the classified contract. The competent security authority of the contract owner shall also transmit, or arrange for the transmission of, this classification guide to the competent security authority of the contractor.

(4) The competent security authority of the contract owner shall ensure that the contractor will be granted access to classified information only after the pertinent Facility Security Clearance has been received from the competent security authority of the contractor.

Article 8
Transmission of Classified Information

(1) Classified information at the VRLO TAJNO / STRENG GEHEIM level shall only be transmitted between the Contracting Parties through Government-to-Government channels in accordance with the respective national laws and regulations.

(2) As a matter of principle, classified information at the POVJERLJIVO / VS-VERTRAULICH and TAJNO / GEHEIM levels shall be transmitted from one state to another by official courier. The competent security authorities of the Contracting Parties may agree on alternative channels of transmission. Classified information shall be forwarded to the recipient in accordance with national laws and regulations, and receipt of classified information shall be confirmed by, or at the instance of, the competent authority.

(3) The competent security authorities of the Contracting Parties may agree – generally or subject to restrictions – that classified information at the POVJERLJIVO / VS-VERTRAULICH and TAJNO / GEHEIM levels may be transmitted through channels other than official courier. In such cases,

1. the bearer must be authorised to have access to classified information of the equivalent classification level,

2. a list of the items of classified information transmitted must be retained by the sender; a copy of this list shall be handed over to the recipient for forwarding to the competent authority,

3. items of classified information must be packed in accordance with the regulations governing transportation within national boundaries,

4. items of classified information must be delivered against receipt, and

5. the bearer must carry a courier certificate issued by the competent authority of the sender.

(4) Where classified information has to be transmitted, the means of transportation, the route, and in case of need an escort shall be determined on a case-by-case basis by the competent security authorities on the basis of a detailed transport plan.

(5) As an additional alternative means of transmission, classified information up to and including the POVJERLJIVO / VS-VERTRAULICH level can be transmitted through non-cleared private courier services provided that the following conditions are met:

1. The courier service is located within the territory of one of the states of the Contracting Parties and has established a protective security programme for handling valuable items with a signature service, including a record of continuous accountability on custody through either a signature and tally record, or an electronic tracking or tracing system.

2. The courier service must obtain and provide proof of delivery on the signature and tally record to the sender, or it must obtain receipts against package numbers.

3. The courier service must guarantee that the consignment will be delivered to the recipient by a specific time and date within a 24-hour period.

4. The courier service may charge a commissioner or sub-contractor. However, the responsibility for fulfilling the above requirements must remain with the courier service.

(6) Classified information at the VRLO TAJNO / STRENG GEHEIM level shall not be transmitted electronically.

(7) Classified information at the POVJERLJIVO / VS-VERTRAULICH and TAJNO / GEHEIM levels may be transmitted electronically in encrypted form only. Classified information of these classification levels may only be encrypted by encryption means approved by mutual agreement by the competent security authorities of the Contracting Parties.

(8) Classified information at the OGRANIČENO / VS-NUR FÜR DEN DIENSTGEBRAUCH level may be transmitted by post or other delivery services to recipients within the territory of the state of the other Contracting Party, taking into account national laws and regulations.

(9) Classified information at the OGRANIČENO / VS-NUR FÜR DEN DIENSTGEBRAUCH level may be transmitted electronically or made accessible by means of commercial encryption devices approved by a competent security authority of the originating Contracting Party. Classified information of this classification level may only be transmitted in an unencrypted form if this is not contrary to national laws and regulations, no approved encryption means are available, transmission is effected within fixed networks only and the sender and the recipient have reached agreement on the proposed transmission in advance.

Article 9
Visits

(1) As a matter of principle, it is only with the prior permission of the competent security authority of the Contracting Party whose state is to be visited that visitors from the state of

one Contracting Party will, in the state of the other Contracting Party, be granted access to classified information and to facilities whose personnel handles classified information. Such permission shall be given only to persons having a need-to-know and – except in the case of classified information at the OGRANIČENO / VS-NUR FÜR DEN DIENSTGEBRAUCH level – having been authorised to have access to classified information.

(2) Requests for visits shall be submitted, on a timely basis and in accordance with the laws and regulations of the Contracting Party's state whose territory such visitors wish to enter, to the competent security authority of that state. The competent security authorities shall inform each other of the details regarding such requests and shall ensure that personal data are protected.

(3) Requests for visits shall be submitted in the language of the state to be visited or in English and shall contain the following information:

1. the visitor's first name and surname, date and place of birth, and his passport or identity card number;
2. the visitor's citizenship;
3. the visitor's service designation, and the name of his parent authority or agency;
4. the level of the visitor's security clearance for access to classified information;
5. the purpose of the visit, and the proposed date of the visit; and
6. the designation of the agencies, the contact persons and the facilities to be visited.

Article 10
Consultations and Settlement of Disputes

(1) The Contracting Parties shall take note of the laws and regulations governing the protection of classified information that apply within the state of the other Contracting Party.

(2) To ensure close cooperation in the implementation of this Agreement, the competent authorities of the Contracting Parties shall consult each other at the request of one of these authorities.

(3) Each Contracting Party shall, in addition, allow the competent security authority of the other Contracting Party or any other authority designated by mutual agreement to visit the territory of its state in order to discuss, with the competent authorities of its state, the procedures and facilities for the protection of classified information received from the other Contracting Party. Each Contracting Party shall assist that authority in ascertaining whether such classified information received from the other Contracting Party is adequately protected. The details of the visits shall be laid down by the competent authorities.

(4) Any dispute between the Contracting Parties arising from the interpretation or application of this Agreement shall be resolved solely by consultations or negotiations between the Contracting Parties and shall not be referred to any national or international tribunal or third party for settlement.

Article 11
Violation of Provisions Governing the Protection of Classified Information

(1) Whenever unauthorised disclosure of classified information cannot be ruled out or if such disclosure is suspected or ascertained, the other Contracting Party shall immediately be informed either in the national language of the authority to be informed or in English.

(2) Violations of provisions governing the protection of classified information shall be investigated, and pertinent legal action shall be taken, by the competent authorities and courts in the state of the Contracting Party having jurisdiction, according to the law of that state. The other Contracting Party should, if so requested, support such investigations and shall be informed of the outcome.

(3) When a violation has occurred during transmission and before the delivery has been confirmed, the competent security authority of the originating Contracting Party shall take the appropriate actions to investigate and take pertinent legal action.

Article 12
Costs

Each Contracting Party shall pay the expenses incurred by it in implementing the provisions of this Agreement.

Article 13
Competent Security Authorities

The Contracting Parties shall inform each other in writing about the details of their respective competent security authorities immediately after the Agreement has entered into force and shall also provide updates to these details as necessary.

Article 14
Relationship with Other Instruments, Agreements and Memoranda of Understanding

Any existing instruments, agreements and memoranda of understanding between the Contracting Parties or the competent security authorities on the protection of classified information shall be unaffected by this Agreement in so far as they do not conflict with its provisions.

Article 15

Final Provisions

(1) This Agreement shall enter into force on the date on which the Government of the Republic of Croatia has notified the Government of the Federal Republic of Germany that the national requirements for the entry into force have been fulfilled. The relevant date shall be the date of receipt of the notification.

(2) This Agreement is concluded for an indefinite period of time.

(3) This Agreement may be amended in writing by mutual agreement between the Contracting Parties. Either Contracting Party may at any time submit a written request for the amendment of this Agreement. If such a request is submitted by one of the Contracting Parties, the Contracting Parties shall initiate negotiations on the amendment of the Agreement.

(4) Either Contracting Party may at any time, through diplomatic channels, denounce this Agreement by giving six months' written notice. In the event of denunciation, classified information transmitted, or generated by the contractor, on the basis of this Agreement shall continue to be treated in accordance with the provisions of Article 4 above for as long as is justified by the existence of the security classification.

(5) Registration of this Agreement with the Secretariat of the United Nations, in accordance with Article 102 of the Charter of the United Nations, shall be initiated by the Contracting Party in the state of which the Agreement is concluded immediately following its entry into force. The other Contracting Party shall be informed of registration, and of the UN registration number, as soon as this has been confirmed by the Secretariat of the United Nations.

(6) The Agreement between the Ministry of Defence of the Republic of Croatia and the Federal Ministry of Defence of the Federal Republic of Germany concerning the Mutual Protection of Classified Military Information signed on 28 April 2003 shall cease to have

effect upon the date of entry into force of this Agreement. Upon the entry into force of this Agreement, classified military information transmitted, or generated by the contractor, on the basis of the Agreement of 28 April 2003 shall be treated in accordance with the provisions of this Agreement for as long as is justified by the existence of the security classification.

Done at Zagreb on 18 April 2023 in two originals in the Croatian, German and English languages, all texts being authentic. In case of divergent interpretations of the Croatian and German texts, the English text shall prevail.

For the Government of
the Republic of Croatia

For the Government of
the Federal Republic of Germany