

**AGREEMENT
BETWEEN
THE AUSTRIAN FEDERAL GOVERNMENT
AND
THE GOVERNMENT OF THE REPUBLIC OF CROATIA
ON THE EXCHANGE AND MUTUAL PROTECTION
OF CLASSIFIED INFORMATION**

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

Intending to ensure the security of all classified information designated and marked as such in accordance with national laws and regulations of either Party and transmitted to the other Party,

Wishing to provide rules for the mutual protection of classified information transmitted or generated in the course of the cooperation between the Parties,

Have agreed upon the following:

**ARTICLE 1
DEFINITIONS**

For the purposes of this Agreement:

- a) "Classified Information" means any information, regardless of its form, designated and marked as such in accordance with the national laws and regulations of either Party in order to ensure protection against unauthorized disclosure, misappropriation or loss;
- b) "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;
- c) "Competent Authority" means the National Security Authority and any other competent authority and agency notified in accordance with Article 13 of this Agreement;
- d) "Personnel Security Clearance" means the determination by a Competent Authority that an individual is eligible to have access to Classified Information in accordance with national laws and regulations;
- e) "Facility Security Clearance" means the determination by a Competent Authority that a legal entity has the physical and organizational capability to meet the conditions

for access to and handling of Classified Information in accordance with national laws and regulations;

f) "Classified Contract" means a contract or subcontract between a legal entity or individual from the State of one Party and a legal entity or individual from the State of the other Party, the implementation of which requires access to Classified Information or its generation;

g) "Originator" means the originating Party as well as any legal entity or individual under its jurisdiction which releases Classified Information;

h) "Recipient" means the receiving Party as well as any legal entity or individual under its jurisdiction which receives Classified Information;

i) "Third Party" means a legal entity or an individual which is not an Originator or Recipient of the Classified Information transmitted in accordance with this Agreement, a government not Party to this Agreement or an international organisation;

j) "Breach of Security" 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.

ARTICLE 2 SECURITY CLASSIFICATION LEVELS

The Parties agree on the equivalence of the following security classification levels:

Republic of Croatia:	Republic of Austria:	Corresponding English expression:
VRLO TAJNO	STRENG GEHEIM	TOP SECRET
TAJNO	GEHEIM	SECRET
POVJERLJIVO	VERTRAULICH	CONFIDENTIAL
OGRANIČENO	EINGESCHRÄNKT	RESTRICTED

ARTICLE 3 MARKING

(1) Classified Information to be transmitted shall be marked by the Originator in accordance with the appropriate Security Classification Level. The Recipient shall mark received Classified Information with the Security Classification Level equivalent to the marking by the Originator.

(2) Classified Information generated, reproduced or translated in the course of cooperation under this Agreement shall also be marked.

(3) The Security Classification Level shall only be altered or revoked with the written consent of the Originator. The Originator shall inform the Recipient without delay

about any alteration or revocation of the security classification level of the transmitted Classified Information.

ARTICLE 4

PRINCIPLES OF THE PROTECTION OF CLASSIFIED INFORMATION

(1) The Parties shall take all appropriate measures to ensure the protection of the transmitted Classified Information and shall provide for the necessary control of this protection.

(2) The Parties shall afford transmitted Classified Information at least the same level of protection as they afford their own Classified Information of the equivalent Security Classification Level.

(3) Transmitted Classified Information shall only be used for the purpose it has been released for.

(4) Transmitted 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 require this access for the exercise of their duties.

(5) A Party shall not make Classified Information accessible to a third party without the prior written consent of the Competent Authority of the Originator.

(6) Classified Information generated in the course of cooperation under this Agreement shall enjoy the same protection as Classified Information transmitted in the course of cooperation under this Agreement.

ARTICLE 5

PERSONNEL SECURITY CLEARANCE

(1) Within the scope of this Agreement, each Party shall recognize the Personnel Security Clearances issued by the other Party.

(2) 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.

(3) Within the scope of this Agreement, the Competent Authorities shall inform each other without delay about any alteration with regard to Personnel Security Clearances, in particular about a revocation or an alteration of the Security Classification Level.

(4) Upon request of the Competent Authority of the Originator, the Competent Authority of the Recipient shall issue a written confirmation that an individual is authorized to access Classified Information.

ARTICLE 6 CLASSIFIED CONTRACTS

- (1) A Classified Contract shall contain provisions on the security requirements and on the Security Classification Level of the information to be released. A copy of the provisions shall be sent to the Competent Authority.
- (2) In the context of Classified Contracts, each Party shall recognize the Facility Security Clearances issued by the other Party.
- (3) In the context of the preparation or conclusion of Classified Contracts, the Competent Authorities shall inform each other upon request whether a valid Facility Security Clearance has been issued or the relevant proceedings have been initiated and about the security requirements for the Classified Information involved.
- (4) The Competent Authorities shall inform each other about any Classified Contracts falling under this Agreement.
- (5) The Competent Authorities shall inform each other without delay about any alteration with regard to Facility Security Clearances falling under this Article, in particular about a revocation or an alteration of the Security Classification Level.
- (6) The Originator shall transmit to the Recipient and to the Competent Authority of the Recipient a list of the Classified Information to be transmitted under the Classified Contract.
- (7) A contractor may hire a subcontractor to fulfil a part of a Classified Contract. Subcontractors shall be subject to the same security requirements as those applicable for the contractor.

ARTICLE 7 TRANSMISSION

Classified Information shall be transmitted through diplomatic channels or any other channels as agreed upon between the Parties. Receipt of Classified Information marked POVJERLJIVO / VERTRAULICH / CONFIDENTIAL and above shall be acknowledged in writing. Upon the request of the Originator, receipt of Classified Information marked OGRANIČENO / EINGESCHRÄNKT / RESTRICTED shall also be acknowledged in writing.

ARTICLE 8 REPRODUCTION AND TRANSLATION

- (1) The reproduction and translation of Classified Information may be restricted or excluded by the Originator. The number of copies shall be restricted to that required for official purposes.

(2) Classified Information marked as VRLO TAJNO / STRENG GEHEIM / TOP SECRET shall not be reproduced or translated without the prior written consent of the Originator.

(3) Classified Information shall only be translated by persons authorized to have access to Classified Information of the respective Security Classification Level.

(4) Copies and translations shall be protected in the same way as originals. The translation shall bear an appropriate note in the language into which it is translated that the translation contains Classified Information of the Originator.

ARTICLE 9 DESTRUCTION

(1) Classified Information shall be destroyed in a manner that does not permit a full or partial reconstruction. The destruction of Classified Information that has been registered in accordance with national laws and regulations shall be recorded.

(2) The Originator may, by additional marking or sending subsequent written notice to the Recipient, expressly prohibit the destruction of Classified Information. If the destruction of Classified Information is prohibited, it shall be returned to the Originator.

(3) In case of a 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 Recipient shall inform the Competent Authority of the Originator about this destruction as soon as possible.

ARTICLE 10 VISITS

(1) Visits requiring access to Classified Information are subject to prior permission by the Competent Authority of the host Party. The permission shall be granted only to persons authorized in accordance with national laws and regulations to have access to Classified Information of the respective Security Classification Level.

(2) Requests for visits shall be submitted to the Competent Authority of the host Party at least ten working days prior to the visit, in urgent cases within a shorter period. The Competent Authorities shall inform each other about the details of the visit and ensure the protection of personal data.

(3) Requests for visits shall be made in English language and shall state in particular the following:

- a) purpose and proposed date of the visit;
- b) first name and family name, date and place of birth, citizenship and passport or ID card number of the visitor;
- c) position of the visitor and name of the authority, agency or enterprise represented;

- d) validity and level of the Personnel Security Clearance of the visitor;
- e) name, address, phone and fax number, e-mail address and point of contact of the authorities, agencies or facilities to be visited;
- f) date of the request and signature of the Competent Authority.

(4) The Competent Authorities of the Parties may draw up lists of individuals authorised 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 the event of a Breach of Security, the Competent Authority of the Recipient shall immediately inform the Competent Authority of the Originator in writing.

(2) Violations of the provisions on the protection of Classified Information falling under this Agreement shall be investigated and prosecuted in accordance with national laws and regulations. The Parties shall assist each other upon request.

(3) The Parties shall inform each other about the result of the investigations and the measures taken.

ARTICLE 12 EXPENSES

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

ARTICLE 13 COMPETENT AUTHORITIES

The Parties shall notify each other through diplomatic channels of the Competent Authorities responsible for the implementation of this Agreement.

ARTICLE 14 CONSULTATIONS

(1) The Competent Authorities shall inform each other of the respective national laws and regulations on the protection of Classified Information and any significant amendments thereof.

(2) In order to ensure close cooperation in the implementation of this Agreement, the Competent Authorities shall consult each other and facilitate the necessary mutual visits.

ARTICLE 15
SETTLEMENT OF DISPUTES

Any dispute regarding the application or interpretation of this Agreement shall be resolved by direct consultations and negotiations between the Parties.

ARTICLE 16
FINAL PROVISIONS

(1) This Agreement is concluded for an indefinite period of time and shall enter into force on the first day of the second month following the day on which the Parties have notified each other in writing, through diplomatic channels, of the completion of the internal procedures necessary for the entry into force of this Agreement.

(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) Each Party may terminate this Agreement at any time by giving written notice to the other Party through diplomatic channels. In such a case, the Agreement shall terminate six months after the receipt of the termination notice by the other Party. In the case of termination, all Classified Information transmitted or generated in application of this Agreement shall continue to be protected in accordance with the provisions set forth in this Agreement.

Done at... on ... in two originals in the Croatian, German and English languages, all texts being equally authentic. In case of any divergence of interpretation, the English text shall prevail.

For the Austrian Federal Government **For the Government of
the Republic of Croatia**