

**AGREEMENT
BETWEEN
THE GOVERNMENT OF THE SLOVAK REPUBLIC
AND
THE GOVERNMENT OF THE REPUBLIC OF AZERBAIJAN
CONCERNING THE EXCHANGE AND MUTUAL PROTECTION
OF
CLASSIFIED INFORMATION**

**THE GOVERNMENT OF THE SLOVAK REPUBLIC
AND
THE GOVERNMENT OF THE REPUBLIC OF AZERBAIJAN,**

Hereinafter jointly referred to as “the Parties”, and each individually as “Party”,

In order to ensure the mutual protection of Classified Information, considering the national security interests of their States, have agreed upon the following:

ARTICLE 1 PURPOSE AND SCOPE

1. The purpose of this Agreement is to ensure the protection of Classified Information either exchanged between the Parties or between Contractors under their jurisdiction, or created (in the framework of a bilateral program) under this Agreement. This Agreement sets out the security procedures and arrangements for such protection.
2. The Parties shall take all appropriate measures under the national legislation of their States to ensure the protection of Classified Information in accordance with this Agreement.
3. This Agreement does not constitute a basis to compel the provision or exchange of Classified Information by the Parties.

ARTICLE 2 DEFINITIONS

For the purpose of this Agreement, the following definitions mean:

- a) **“Classified Contract”** means any legally enforceable agreement to be entered into by one Party or a Contractor under its jurisdiction with the other Party or a Contractor under its jurisdiction, which contains Classified Information or the performance of which requires access or potential access to creation, use or transfer of Classified Information.
- b) **“Classified Information”** means any information, material or object, regardless its form or nature, or any parts thereof, marked with a security classification level by one of the Parties, the unauthorised disclosure, alteration, compromise or loss of which could cause varying degrees of damage or harm to the interests of one or both of the Parties.
- c) **“Competent Security Authority”** means the government authority of a Party responsible for the implementation and supervision of this Agreement. The Parties may delegate part of the responsibilities of the Competent Security Authority under this Agreement to a delegated competent security authority.
- d) **“Contractor”** means any individual, legal entity or other forms of organisation under the jurisdiction of a Party, entering into or otherwise bound by a Classified Contract.
- e) **“Facility Security Clearance”** means the positive determination by the Competent Security Authority that a facility has in place appropriate security measures to access and handle Classified Information up to and including a specified security classification level, in accordance with the national legislation of its State.

- f) **“Personnel Security Clearance”** means the positive determination by the Competent Security Authority that an individual has been security cleared to access and handle Classified Information up to and including a specified classification level, in accordance with the national legislation of its State.
- g) **“Need-to-Know”** means the requirement for an individual, legal entity or other form of organisation, to access, have knowledge of, or possess Classified Information in order to be able to perform their official tasks or service.
- h) **“Originating Party”** means a Party or a Contractor under its jurisdiction, which creates and/or provides Classified Information to the Receiving Party under this Agreement.
- i) **“Receiving Party”** means a Party or a Contractor under its jurisdiction, which receives Classified Information from the Originating Party under this Agreement.
- j) **“Security Classification Guide”** means a document associated with a Classified Contract specifying the applicable security classification levels of each part of that Classified Contract.
- k) **“Security Incident”** means any unauthorised disclosure, alteration, compromise, loss, access, handling, storage or destruction of Classified Information, contrary to national legislation of the States of the Parties and/or this Agreement.
- l) **“Third Party”** means any international organisation, government or state, including individuals, legal entities or other forms of organisation under its jurisdiction, which is not a Party to this Agreement.
- m) **“Visits”** means an access to public and private facilities that involve access or potential access to and handling of Classified Information for the purposes of this Agreement.

ARTICLE 3 COMPETENT SECURITY AUTHORITIES

1. Competent Security Authorities are:

For the Slovak Republic:
National Security Authority of the Slovak Republic
Budatinska 30
851 06 Bratislava
Slovak Republic

For the Republic of Azerbaijan:
State Security Service of the Republic of Azerbaijan
14 Parliament Avenue, Baku, AZ 1009
Republic of Azerbaijan

2. The Competent Security Authorities shall provide each other with official contact details.
3. The Parties shall inform each other via diplomatic channels about changes in the contact details of the Competent Security Authorities referred to in paragraph 1, as well as about changes in the contact details of the delegated competent security authorities under this Agreement, where applicable.

ARTICLE 4 SECURITY CLASSIFICATION LEVELS

1. The following security classification levels of the Parties are equivalent and correspond to the security classification levels specified in the national legislation of the States of the Parties.

For the Slovak Republic	For the Republic of Azerbaijan	Equivalent in English
PRÍSNE TAJNÉ	XÜSUSİ ƏHƏMİYYƏTLİ	TOP SECRET
TAJNÉ	TAM MƏXFİ	SECRET
DÔVERNÉ	MƏXFİ	CONFIDENTIAL
VYHRADENÉ	-----	RESTRICTED

2. Information received from the Slovak Republic classified as VYHRADENÉ/-----/RESTRICTED shall be protected as DÔVERNÉ/MƏXFİ/CONFIDENTIAL in the Republic of Azerbaijan.

ARTICLE 5 SECURITY MEASURES

1. The Receiving Party shall mark all the Classified Information that it has received from the Originating Party or that it has created under this Agreement with the security classification level that corresponds to the security classification level given by the Originating Party in accordance with the scheme contained in Article 4 and, where applicable, in accordance with paragraph 4 of this Article.
2. The Receiving Party shall not modify or revoke the security classification level of received or created Classified Information under this Agreement without the written

approval of the Originating Party.

3. The Originating Party shall ensure that the Receiving Party is informed of any change in the security classification level of the Classified Information provided.
4. The Originating Party may additionally mark the Classified Information with handling requirements, to specify any limitations on its use, disclosure, release and access by the Receiving Party.
5. Classified Information jointly created by the Parties shall be assigned a security classification level that is mutually determined by the Parties.
6. The Parties shall afford Classified Information exchanged or created under this Agreement at least the same protection as they afford to their own Classified Information at the corresponding security classification level.
7. In accordance with Article 1, paragraph 2 of this Agreement, the Parties shall take all appropriate measures to ensure that the Originating Party:
 - a) marks Classified Information with the appropriate security classification level in accordance with the national legislation of its State;
 - b) informs the Receiving Party of any conditions of release or limitations on the use of the Classified Information provided.
8. In accordance with Article 1, paragraph 2 of this Agreement, the Parties shall take all appropriate measures to ensure that the Receiving Party:
 - a) affords the same level of protection to Classified Information as afforded to its national Classified Information of an equivalent security classification level;
 - b) ensures that Classified Information is not disclosed or released to a Third Party without the prior written consent of the Originating Party;
 - c) uses Classified Information solely for the purpose it has been released for and in accordance with handling requirements of the Originating Party.

ARTICLE 6

ACCESS TO CLASSIFIED INFORMATION

1. Access to Classified Information shall be granted only to individuals on a Need-to-know basis, who are briefed on their responsibilities for the protection of Classified Information, and have signed a non-disclosure agreement in accordance with the national legislation of the State of the Receiving Party.
2. In addition to the requirements in paragraph 1 of this Article, access to Classified Information at the security classification levels equivalent to “DÔVERNÉ/MÔXFÎ/CONFIDENTIAL” and above as mentioned in Article 4 of this Agreement, shall be granted only to those individuals who hold a Personnel Security

Clearance at the corresponding level or who are otherwise duly authorised to access Classified Information by virtue of their function, in accordance with the national legislation of the State of the Receiving Party.

ARTICLE 7

CLASSIFIED CONTRACTS AND ACCESS TO FACILITIES

1. Upon request of the Originating Party, the Competent Security Authority of the Receiving Party shall inform the Competent Security Authority of the Originating Party whether a Contractor, under jurisdiction of the Receiving Party and participating in a Classified Contract or precontractual negotiations regarding a Classified Contract, has been issued a Facility Security Clearance at the required security classification level. If the Contractor does not, at that point, hold a Facility Security Clearance, or the Facility Security Clearance is at a lower level than that required, the Competent Security Authority receiving the request shall inform the requesting Competent Security Authority of that fact.
2. If a Party or a Contractor under its jurisdiction proposes to grant a Classified Contract at a security classification level equivalent to “DÔVERNÉ/MƏXFİ/CONFIDENTIAL” or above as mentioned in Article 4 of this Agreement, with the (sub-) Contractor under the jurisdiction of the other Party, it shall first obtain written confirmation from the Competent Security Authority of the other Party that the Contractor has been granted a Facility Security Clearance at the appropriate security classification level. For Classified Contracts at the security classification level equivalent to “VYHRADENÉ/-----/RESTRICTED” as mentioned in Article 4 of this Agreement, a Facility Security Clearance may be required, if mandated by national legislation of the State of the Contractor.
3. In accordance with Article 1, paragraph 2 of this Agreement, the Party under whose jurisdiction the Classified Contract is to be performed shall ensure that the Contractor:
 - a) ensures that all individuals granted access to Classified Information are informed of their responsibilities to protect Classified Information in accordance with the conditions defined in this Agreement and in accordance with the national legislation of their States;
 - b) monitors the security conduct within its facilities;
 - c) notifies promptly its Competent Security Authority of any Security Incident relating to the Classified Contract.
4. In addition to Article 7, paragraph 3, subparagraphs a, b and c of this Agreement, for Classified Contracts at the security classification levels equivalent to “DÔVERNÉ/MƏXFİ/CONFIDENTIAL” or above as mentioned in Article 4 of this Agreement, the Competent Security Authority shall ensure that the Contractor holds

a Facility Security Clearance at the appropriate security classification level in order to protect the Classified Information and that the individuals requiring access to Classified Information hold a Personnel Security Clearance at the appropriate security classification level.

5. Every Classified Contract shall include security requirements which identify the following aspects:
 - a) a Security Classification Guide;
 - b) a procedure for communication of changes in the security classification level, taking into account Article 5, paragraph 3 of this Agreement;
 - c) the channels and procedures to be used for the transport and/or transmission of Classified Information;
 - d) instructions for the handling, storage, destruction and returning of Classified Information;
 - e) contact details of the Competent Security Authorities responsible for overseeing the protection of Classified Information related to the Classified Contract;
 - f) the obligation to notify any Security Incidents to the Competent Security Authority of the Contractor and the obligation for Contractors to take all reasonable steps to assist in mitigating the effect of such a security violation, in consultation with the Competent Security Authority;
 - g) in case a Classified Contract in whole or in part is sub-contracted to a sub-Contractor, the obligation to impose all the stipulations concerning Contractors in this Agreement to the sub-Contractor;
 - h) a reference to this Agreement;
 - i) a statement that Classified Information exchanged or created pursuant to the Classified Contract shall be protected by the Contractor in accordance with this Agreement and applicable national legislation.
6. The Competent Security Authority of the Party or the Contractor under its jurisdiction awarding the Classified Contract shall forward a copy of the security requirements to the Competent Security Authority of the Receiving Party to facilitate the security oversight of the Classified Contract.
7. The procedures for the approval of visits associated with Classified Contract activities by personnel of one Party to the other Party, shall be in accordance with Article 8 of this Agreement.

ARTICLE 8

VISITS

1. Visits requiring access to Classified Information at a security classification level equivalent to “DÔVERNÉ/MƏXFİ/CONFIDENTIAL” or above as mentioned in Article 4 of this Agreement are subject to the prior written consent of the Competent Security Authority of the host Party, unless otherwise agreed between the Competent

Security Authorities. Such consent shall be given only to individuals on a Need-to-Know basis who hold a valid Personnel Security Clearance to the appropriate level or who are otherwise duly authorised to access Classified Information by virtue of their function, in accordance with the national legislation of the State of the Receiving Party. If mandated by national legislation of the State of the host Party, “VYHRADENÉ/-----/RESTRICTED” level visits may be subject to the prior written consent of the Competent Security Authority of the host Party.

2. The visitor shall submit the request for a visit at least ten calendar days in advance of the proposed date of the visit to the Competent Security Authority of his Party, which shall forward it to the Competent Security Authority of the other Party. In urgent cases, the Competent Security Authorities may agree on a shorter period.
3. Request for visit shall include:
 - a) full name of the visitor, date and place of birth, nationality and passport/ID card number;
 - b) official title and present position of the visitor and name of the organisation the visitor represents or to which the visitor belongs;
 - c) confirmation of the visitor’s Personnel Security Clearance and its level and validity;
 - d) date and duration of the visit. In the case of recurring visits the total period covered by the visits shall be stated;
 - e) purpose of the visit and the anticipated highest security classification level of Classified Information to be discussed or accessed;
 - f) name, address, phone number, e-mail address and point of contact of the facility to be visited;
 - g) dated and stamped signature of a representative of the visitor’s Competent Security Authority.
4. The Competent Security Authorities may agree on a list of visitors entitled to recurring visits for a period not exceeding twelve months. The Competent Security Authorities shall agree on the further details of the recurring visits.
5. The Competent Security Authority of the host Party shall inform the security officials of the organisation to be visited, of the details of those individuals whose visit request has been approved. Once approval has been given, visit arrangements for individuals who have been given approval for recurring visits may be made directly with the agency, facility or organisation concerned.
6. Classified Information provided to or acquired by a visitor shall be handled in accordance with the provisions of this Agreement.
7. The Parties shall ensure, pursuant to the national legislation of their States, the protection of the personal data of the individuals requesting for a visit requiring

access to Classified Information. This personal data shall not be used for any other purpose than determining on the request for (recurring) visits.

ARTICLE 9 TRANSMISSION OF CLASSIFIED INFORMATION

1. Classified Information shall be transmitted to the Receiving Party in accordance with the national legislation of the State of the Originating Party or as otherwise agreed in writing between the Competent Security Authorities.
2. Electronic transmission of Classified Information may take place only by using cryptographic means in accordance with procedures to be approved by the Competent Security Authorities.
3. The Receiving Party shall confirm the receipt of Classified Information in writing.

ARTICLE 10 REPRODUCTION, TRANSLATION AND DESTRUCTION OF CLASSIFIED INFORMATION

1. Reproductions and translations of Classified Information shall be marked and placed under the same protection as the original Classified Information.
2. Reproductions and translations shall be limited to the minimum required for use under this Agreement.
3. Translations shall contain a suitable annotation in the language of translation, indicating that they contain Classified Information of the Originating Party.
4. Classified Information marked at the security classification level equivalent to “PRÍSNE TAJNÉ/XÜSUSÍ ƏHƏMİYYƏTLİ/TOP SECRET” as mentioned in Article 4 of this Agreement, shall not be reproduced or translated without the prior written consent of the Originating Party.
5. Classified Information marked at the security classification level equivalent to “PRÍSNE TAJNÉ/XÜSUSÍ ƏHƏMİYYƏTLİ/TOP SECRET” as mentioned in Article 4 of this Agreement, shall be destroyed only with the prior written consent of the Originating Party. It shall be returned to the Originating Party after it is no longer considered necessary by the Receiving Party.
6. Classified Information marked up to and including the security classification level equivalent to “TAJNÉ/TAM MƏXFİ/SECRET” as mentioned in Article 4 of this Agreement, shall be destroyed after it is no longer considered necessary by the

Receiving Party.

7. If a crisis situation makes it impossible for a Receiving Party to protect Classified Information provided under this Agreement, the Classified Information shall be destroyed immediately. The Receiving Party shall notify promptly in writing the Competent Security Authority of the Originating Party about the destruction of this Classified Information.

ARTICLE 11 SECURITY CO-OPERATION

1. The Competent Security Authorities shall, on request, inform each other about changes in the national legislation of their States, policies, and practices for protection of Classified Information.
2. On request of the Competent Security Authority of one Party, the Competent Security Authority of the other Party shall issue a written confirmation that a valid Personnel Security Clearance or Facility Security Clearance has been issued.
3. The Competent Security Authorities of the Parties shall recognise Personnel Security Clearances and Facility Security Clearances issued in accordance with the national legislation of the State of the other Party and in the scope of this Agreement.
4. The Competent Security Authorities shall assist each other in carrying out Facility Security Clearance and Personnel Security Clearance vetting procedures on request and in accordance with the national legislation of their States.
5. The Competent Security Authorities shall promptly notify each other in writing about changes in mutually recognised Personnel Security Clearances and Facility Security Clearances.
6. The co-operation under this Agreement shall be effected in English language.

ARTICLE 12 SECURITY INCIDENT

1. In case a Security Incident of Classified Information of the Originating Party is suspected or ascertained by the Receiving Party, it shall inform its Competent Security Authority in writing as soon as possible. The notice must contain sufficient details for the Originating Party to assess the consequences and circumstances of the suspected or actual violation.
2. Competent Security Authorities shall immediately inform each other in writing of any actual or potential Security Incident involving Classified Information.

3. The Receiving Party shall immediately investigate any actual or potential Security Incident. The Competent Security Authority of the Originating Party shall, if required, cooperate in the investigation.
4. The Competent Security Authority of the Receiving Party shall take appropriate measures in accordance with the national legislation of its State to limit the consequences and to prevent a recurrence of the Security Incident. The Competent Security Authority of the Originating Party shall be informed of the outcome of the investigation and, if any, of measures taken.

ARTICLE 13 COSTS

Each Party shall bear its own costs incurred in the course of implementing and executing its obligations under this Agreement, unless otherwise mutually determined by the Parties.

ARTICLE 14 DISPUTE RESOLUTION

Any dispute arising from the interpretation, implementation or application of this Agreement shall be settled exclusively through consultation or negotiations between the Parties and shall not be referred to any national or international tribunal or a Third Party for resolution.

ARTICLE 15 IMPLEMENTING ARRANGEMENTS

The Competent Security Authorities of the Parties may conclude implementing arrangements pursuant to this Agreement.

ARTICLE 16 AMENDMENTS

This Agreement may be amended by mutual written consent of the Parties. Such amendments shall be made in a form of separate protocols being an integral part of this Agreement and shall enter into force in accordance with Article 17, paragraph 1 of this Agreement.

ARTICLE 17 FINAL PROVISIONS

1. This Agreement is concluded for an indefinite period of time. Each Party shall notify

the other Party through diplomatic channels once the national procedures necessary for entry into force of this Agreement have been completed. This Agreement shall enter into force on the first day of the second month following the receipt of the latter notification.

2. Each Party may, at any time, terminate this Agreement by written notification to the other Party through diplomatic channels. In this case, termination shall take effect six months after the receipt of the respective notification.
3. In case of termination of this Agreement, all Classified Information exchanged, released or created under this Agreement shall remain protected in accordance with the terms of this Agreement before it was terminated, for as long as Classified Information remains classified.

IN WITNESS whereof the representatives of the Parties, duly authorised thereto, have signed this Agreement.

Done in on in two original copies each in the Slovak, Azerbaijani 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 Slovak Republic**

**For the Government of
the Republic of Azerbaijan**