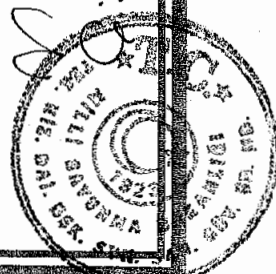
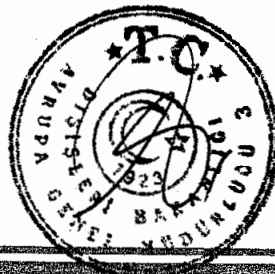
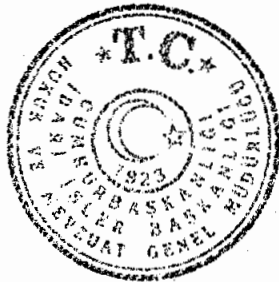


AGREEMENT  
BETWEEN  
THE GOVERNMENT OF THE REPUBLIC OF TURKEY  
AND  
THE GOVERNMENT OF HUNGARY  
ON MUTUAL PROTECTION OF CLASSIFIED  
INFORMATION IN DEFENCE INDUSTRY



## Introduction

The Government of the Republic of Turkey and The Government of Hungary (hereinafter referred to individually as Party, collectively as Parties),

Intending to ensure security of the Classified Information related to defence industry that has been classified in the country of one Party and transferred to the country of the other Party and/or generated by mutual cooperation between the Parties and/or the Authorized Entities in the countries of the Parties,

Desiring to lay down the procedures and principles for ensuring the security of the Classified Information related to the Classified Contracts concluded in the framework of defence industry cooperation between the Parties and/or the Authorized Entities in the countries of the Parties, during their mutual protection and exchange and/or joint production,

Subject to the national legislations of the Parties,

Confirming that this Agreement shall not affect the obligations arising from other international agreements to which either country is a party and shall not be used against the interests, security and territorial integrity of other states,

HAVE AGREED AS FOLLOWS:

### ARTICLE 1

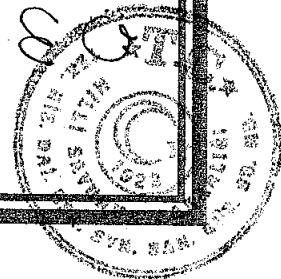
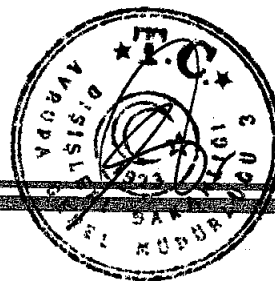
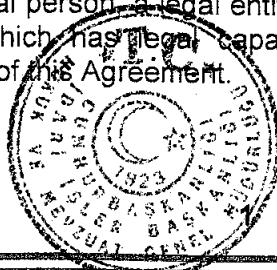
#### PURPOSE AND SCOPE

The purpose of this Agreement is to establish the procedures and principles for ensuring security of the Classified Information related to defence industry in the scope of cooperation activities carried out between the Competent Security Authorities and/or the Authorized Entities in the countries of the Parties in accordance with their respective national legislations.

### ARTICLE 2

#### DEFINITIONS

- 1. Classified Information** – means any information related to defence industry, irrespective of its form, carrier and manner of recording, including documents and material, also in the process of being generated, which require protection against unauthorized disclosure in accordance with the national legislation of either Party and this Agreement.
- 2. Competent Security Authority** – means the national authority authorised on defence industry or the protection of classified information and responsible for implementation of this Agreement, as specified in Article 3 of this Agreement.
- 3. Classified Contract** – means a contract, performance of which involves access to Classified Information or originating of such information, in particular one involving any kinds of works, including preparatory activities, related to the purchase and selling of all kinds of vehicles and equipment of war and arms, and important and critical subsystems and parts therein, research and development and every kind of production thereof, service and infrastructure facility and activities thereof.
- 4. Contractor** – means a natural person, a legal entity or other form of organization under the law of one of the Parties, which has legal capacity to perform Classified Contracts in accordance with the provisions of this Agreement.



**5. Principal** – means a natural person, a legal entity or other form of organization under the law of one of the Parties, which has legal capacity to let Classified Contracts to Contractors in accordance with the provisions of this Agreement.

**6. Facility Security Clearance** – means a document issued in accordance with the national legislation of a Party by the Competent Security Authority or other authorized entity confirming that a Contractor has capability to protect Classified Information; in case of sole proprietors acting as Contractors, a Personnel Security Clearance shall be an equivalent of a Facility Security Clearance.

**7. Principle of Need-to-Know**– means the principle according to which a positive determination is made that an individual has a requirement for access to, knowledge of, or possession of information in order to perform official tasks or services.

**8. Authorized Entities** – means the Parties including the government agencies, legal entities or other forms of organizations, as well as natural persons, competent to handle Classified Information in accordance with their respective national legislations.

**9. Originating Party** – means the Party, as well as natural persons, legal entities or other forms of organizations, competent to originate and transmit Classified Information in accordance with the national legislation of its Party.

**10. Recipient Party** – means the Party, as well as natural persons, legal entities or other forms of organizations, competent to receive Classified Information in accordance with the national legislation of its Party.

**11. Personnel Security Clearance** – means a document issued in accordance with the national legislation of a Party by the Competent Security Authority or other authorized entity confirming that an individual has undergone security vetting and is eligible to have access to Classified Information.

**12. Third Party** – any state, including natural persons, legal entities or other forms of organizations under its jurisdiction, or an international organization not being a Party to this Agreement.

### ARTICLE 3

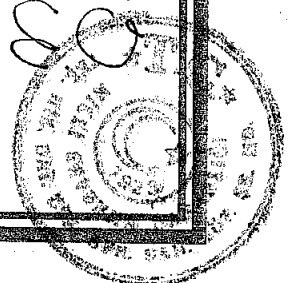
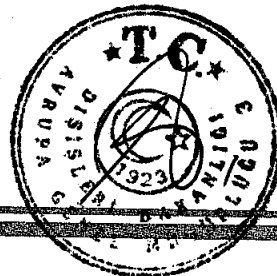
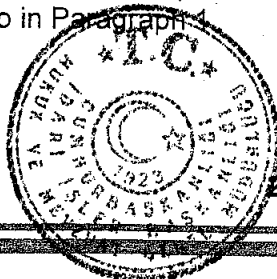
#### COMPETENT SECURITY AUTHORITIES

1. The Competent Security Authorities responsible for implementation of this Agreement are as follows:

- 1) for the Republic of Turkey: Ministry of National Defence of the Republic of Turkey, Technical Services Department;
- 2) for the Republic of Hungary: Ministry for National Economy, State Secretary Economic Development and Regulation.

National Security Authority for the implementation of Article 8 paragraph 1. Article 9 and Article 10.

2. The Parties shall inform each other via diplomatic channels about changes of the Competent Security Authorities referred to in Paragraph 1.



## ARTICLE 4

### SECURITY CLASSIFICATIONS

1. Within the framework of the security measures prescribed by their respective national legislations, the Competent Security Authorities and the Authorized Entities in the countries of the Parties commit to duly ensure the protection of the Classified Information exchanged between each other or generated by mutual cooperation, and adopt the equivalence of levels of classification as shown in the table below, in Turkish, Hungarian and English:

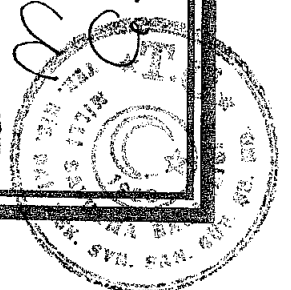
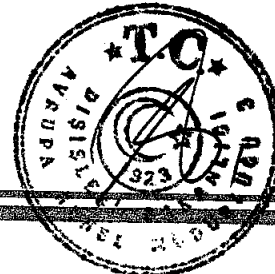
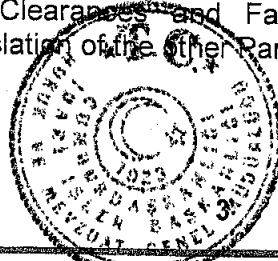
in the Republic of Turkey	In Hungary	equivalent in English
"ÇOK GİZLİ"	„Szigorúan titkos!"	TOP SECRET
"GİZLİ"	„Titkos!"	SECRET
"ÖZEL"	„Bizalmas!"	CONFIDENTIAL
"HİZMETE ÖZEL"	„Korlátozott terjesztésű!"	RESTRICTED

2. The Competent Security Authority and the Authorized Entities of each Party commit to mark the Classified Information they receive from the Competent Security Authority or the Authorized Entities of the other Party, with its own level of national security classification and English equivalent in accordance with the above table.
3. The Competent Security Authorities of the Parties commit to mutually inform each other about the changes made in the security classifications.
4. The level of security classifications given to the Classified Information can be changed or removed only by the Originating Party which has classified them. Such a decision of change or removal shall be immediately notified by the Originating Party to the Recipient Party.

## ARTICLE 5

### PRINCIPLES OF CLASSIFIED INFORMATION PROTECTION

1. The Parties shall adopt every measure provided in this Agreement and subject to their national legislations in order to protect Classified Information transmitted or originated as a result of cooperation between the Parties, including this originated in connection with performance of Classified Contracts.
2. The Classified Information exchanged and/or generated by mutual cooperation between the Competent Security Authorities and/or the Authorized Entities in the countries of the Parties shall be only used in line with the purpose of transfer.
3. The Classified Information shall not be disclosed to a Third Party without prior written consent of the Originating Party.
4. The Classified Information may be disclosed only to persons who have a need-to-know and who are duly authorised in accordance with the national legislation of the Recipient Party.
5. In the scope of this Agreement, the Competent Security Authorities of the Parties shall recognize Personnel Security Clearances and Facility Security Clearances issued in accordance with the national legislation of the other Party.



## ARTICLE 6

### TRANSFER OF THE CLASSIFIED INFORMATION

1. Classified Information shall be transmitted via diplomatic channels or military attaché.
2. Information classified as HİZMETE ÖZEL / „Korlátozott terjesztésű!” / RESTRICTED may be transmitted also through authorized carriers in accordance with the national legislation of the Originating Party.
3. In urgent cases, unless it is possible to use other forms of transmission, if the security requirements defined by the national legislation of the Originating Party are met, the personal carriage of information classified as HİZMETE ÖZEL / „Korlátozott terjesztésű!” / RESTRICTED by authorized individuals is admissible.
4. The Competent Security Authorities of the Parties may agree on other forms of transmitting Classified Information which ensure its protection against unauthorized disclosure in accordance with their respective national legislation.
5. The Recipient Party shall confirm in writing the receipt of Classified Information.

## ARTICLE 7

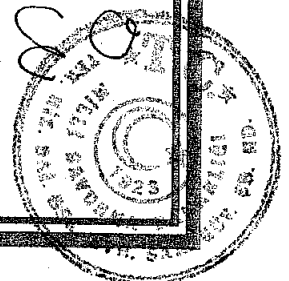
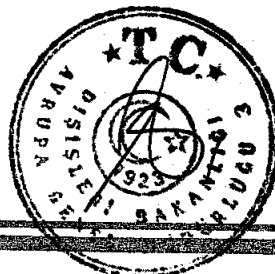
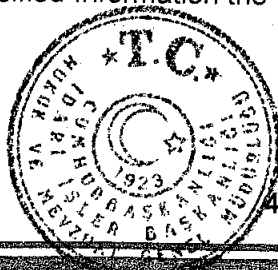
### TRANSLATION, REPRODUCTION AND DESTRUCTION OF THE CLASSIFIED INFORMATION

1. Classified Information marked with the level of security classification of ÇOK GİZLİ / GİZLİ / ÖZEL / „Szigorúan titkos!” / „Titkos!” / „Bizalmas!” / TOP SECRET / SECRET / CONFIDENTIAL shall be translated or reproduced only by prior written consent of the Competent Security Authority of the country of the Originating Party.
2. All translations shall involve an appropriate security classification marking and annotations indicating that the classified document is received from the Originating Party. The translated or reproduced Classified Information shall be subject to the same control and protection as the original information. The number of copies and translations shall be limited to the extent required for official purposes.
3. The information classified as HİZMETE ÖZEL / „Korlátozott terjesztésű!” / RESTRICTED shall be destroyed in accordance with the national legislation of the Recipient Party in a way to prevent re-gathering of the parts either partially or totally. However, the information classified as ÇOK GİZLİ / GİZLİ / ÖZEL / „Szigorúan titkos!” / „Titkos!” / „Bizalmas!” / TOP SECRET / SECRET / CONFIDENTIAL shall be returned by the Recipient Party to the Originating Party instead of being destroyed, when its term or the purpose of usage is ended.

## ARTICLE 8

### CLASSIFIED CONTRACTS

1. Before concluding a Classified Contract, the Principal shall apply to its Competent Security Authority to request that the Competent Security Authority of the other Party confirm that the Contractor is a holder of a valid Facility Security Clearance relevant to the security classification level of the Classified Information the Contractor is to have access to.

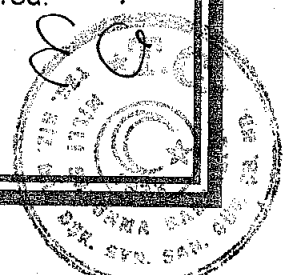
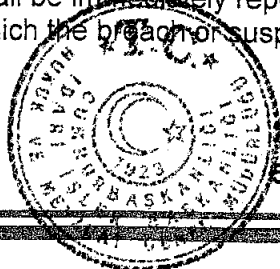


2. Before concluding a Classified Contract involving information classified as HİZMETE ÖZEL / „Korlátozott terjesztésű!” / RESTRICTED, the Competent Security Authority of each Party shall confirm that its Contractor meets security requirements under the national legislation.
3. The confirmation referred to in Paragraphs 1 and 2 shall be tantamount to a guarantee that necessary actions have been conducted in order to declare that the Contractor meets the criteria in the scope of the protection of Classified Information defined in the national legislation of the Party in the territory of which it is located.
4. Classified Information shall not be released to the Contractor until the receipt of the confirmation referred to in Paragraphs 1 and 2.
5. The Principal shall transmit to the Contractor a project security instruction necessary to perform a Classified Contract connected with access to information classified as ÖZEL / „Bizalmas!” / CONFIDENTIAL or above, which is an integral part of such Classified Contract. The project security instruction contains provisions on the security requirements, in particular:
  - 1) the list of types of Classified Information related to a given Classified Contract, including their security classification levels;
  - 2) the rules for granting security classification levels to information originated during the performance of a given Classified Contract.
6. The Principal shall put forward a copy of the project security instruction to the Competent Security Authority of its Party, which shall transmit it to the Competent Security Authority of the Contractor's Party.
7. The performance of a Classified Contract in the part connected with access to Classified Information shall be possible on condition that the Contractor meets the criteria necessary for the protection of Classified Information, pursuant to the project security instruction.
8. Every subcontractor shall comply with the same conditions for the protection of Classified Information as those laid down for the Contractor.
9. Intellectual property rights concerning the Classified Information within the Classified Contracts shall be respected reciprocally in accordance with national legislations. Details and exceptions may be specified in the Classified Contracts.
10. In order to ensure effective cooperation, which is the objective of this Agreement, and in the scope of authority acknowledged by the national legislation of their Parties, the Competent Security Authorities may, if necessary, conclude written detailed technical arrangements.

#### ARTICLE 9

#### BREACH OF SECURITY

1. Breach of security is an action or an omission which is contrary to this Agreement or the national legislation of the Parties concerning Classified Information protection.
2. Information on every breach of security or a suspicion of a breach of security concerning Classified Information of the Originating Party or Classified Information originated as a result of cooperation of the Parties shall be immediately reported to the Competent Security Authority of the Party in the territory of which the breach or suspicion of the breach has occurred.



3. Every breach of security or a suspicion of a breach of security shall be investigated pursuant to the national legislation of the Party in the territory of which it has occurred.

4. In case of a breach of security the Competent Security Authority of the Party in the territory of which the breach has occurred shall inform the Competent Security Authority of the other Party in writing about the fact, circumstances of the breach and the outcome of the actions referred to in Paragraph 3.

5. The Competent Security Authorities of the Parties shall cooperate in the actions referred to in Paragraph 3, upon the request of one of them.

## ARTICLE 10

### VISITS

1. The visits to the facilities of the Authorized Entities in the country of each Party involving access to Classified Information within the scope of cooperation activities between the Competent Security Authorities and/or the Authorized Entities in the countries of the Parties shall be made upon receiving the written authorisation of the Competent Security Authority of the Host Country.

2. The requests for visits shall be notified to the Competent Security Authority of the Host Country in writing, at least 21 (twenty-one) days prior to the proposed date of visit. These requests shall be submitted through the diplomatic channels or military attaché.

3. The form of request for visit shall be prepared for each visit to include the following information below:

a. The Guest Personnel's name and surname, date and place of birth, nationality, passport number and position,

b. The proposed date, programme and anticipated length of visit,

c. The level of the Personnel Security Clearance and type of Classified Information to be accessed as well as the level of security classification,

d. The names of the facilities, premises and places to be visited and the purpose of visit,

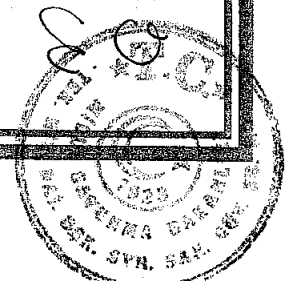
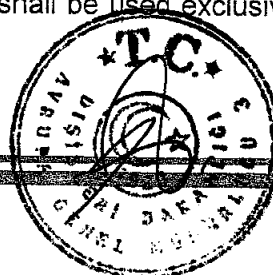
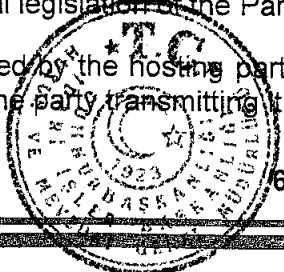
e. The names, surnames and official titles of the persons who will receive the Guest Personnel,

f. The date of request, signature and official stamp of the Competent Security Authority of the country sending the Guest Personnel.

4. A visit permission shall be valid only for the specified date or period. However, in order to facilitate cooperation, a schedule of a visit covering a period not exceeding 12 (twelve) months may be drawn up. In this case, if it is assumed that a planned visit will not end within the allowed period of time and it is necessary to extend the period of such kind of visits, the request for visit shall be renewed by the Competent Security Authority of the country sending the Guest Personnel, at least 21 (twenty-one) days prior to the expiry of the validity of the visit permission in progress.

5. In order to protect personal data referred to in Paragraph 3, the following provisions shall apply, pursuant to the national legislation of the Parties:

a. personal data received by the hosting party shall be used exclusively for the purpose and on condition defined by the party transmitting it;



b. personal data shall be stored by the hosting party no longer than it is necessary for achieving the purpose of its processing;

c. in case of personal data transmitted against the national legislations of the Party, the party transmitting it shall notify the hosting party, which shall be obliged to remove the data in such a manner as to eliminate its partial or total reconstruction;

d. the party transmitting personal data shall take responsibility for its correctness and, in a case the data appears to be untrue or incomplete, shall notify the hosting party, which shall be obliged to correct or remove the data;

e. the hosting party and the party transmitting personal data shall be obliged to register its transmission, receipt and removal;

f. the party transmitting personal data and the hosting party shall be obliged to protect processed personal data efficiently against its disclosure to unauthorized persons, unauthorized modifications of the data, its loss, damage or destruction.

## ARTICLE 11

### LANGUAGES

In the scope of the implementation of the provisions of this Agreement, the Parties shall use English or their official languages, in case of which the translation into the official language of the other Party or English shall be attached.

## ARTICLE 12

### FINANCIAL MATTERS

Each Party shall cover its expenses resulting from the implementation of the provisions of this Agreement.

## ARTICLE 13

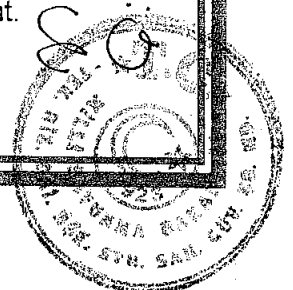
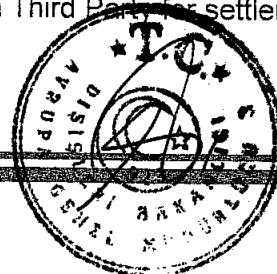
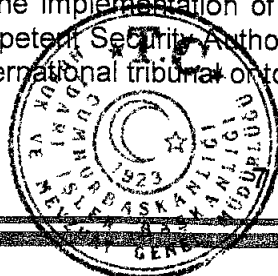
### CONSULTATION AND AMENDMENT

1. Either Party may propose consultation and/or amendment to this Agreement by sending a written notification to the other Party.
2. This Agreement may be amended by mutual written consent of the Parties on the basis of negotiations. The amendments shall enter into force in accordance with the same legal procedure as prescribed under Article 16.
3. The Competent Security Authorities of the Parties shall notify each other of any amendments to their national legislation on the protection of Classified Information concerning implementation of this Agreement.

## ARTICLE 14

### SETTLEMENT OF DISPUTES

1. Any disputes concerning the implementation of this Agreement shall be settled by direct negotiations between the Competent Security Authorities of the Parties. The disputes shall not be referred to any national, international tribunal or to a Third Party for settlement.





2. If settlement of a dispute cannot be reached in the manner referred to in Paragraph 1, such a dispute shall be settled through diplomatic channels. If a solution is not reached within 45 (forty-five) days, each Party may terminate this Agreement.

#### ARTICLE 15

#### EFFECTIVENESS PERIOD AND TERMINATION

1. This Agreement is concluded for 5 (five) years and shall be then automatically renewed for five-year-periods unless terminated with 30 (thirty) days advance notice through diplomatic channels.
2. In case of termination of this Agreement, Classified Information exchanged or originated on the basis of this Agreement shall be protected in accordance with the provisions thereof continuously.


#### ARTICLE 16

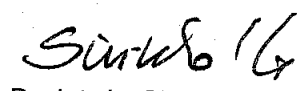
#### ENTRY INTO FORCE

1. This Agreement shall enter into force 30 (thirty) days after the receipt of the last written notification by which the Parties notify each other, through diplomatic channels, of the completion of their internal legal procedures required for the entry into force of the Agreement.
2. This Agreement was signed on 23/11/2017 in Ankara, in two original copies in Turkish, Hungarian and English languages, each copy being equally authentic. In case of any dispute regarding the interpretation of the provisions of this Agreement, the English text shall prevail. In witness whereof, the undersigned, being duly authorized by their respective Governments, have signed this Agreement.

FOR THE GOVERNMENT  
OF THE REPUBLIC OF TURKEY

FOR THE GOVERNMENT  
OF HUNGARY

SIGNATURE :   
NAME : Nurettin CANIKLI  
TITLE : Minister of National Defence

SIGNATURE :   
NAME : Dr. István Simicskó  
TITLE : Minister of Defence

