

TÜRKİYE BÜYÜK MİLLET MECLİSİ BAŞKANLIĞINA

27'nci Yasama Dönemi'nde Başkanlığa sunulmuş olan 2/5027, 2/5038, 2/1781, 2/2783, 2/2278, 2/2935, 2/1897, 2/1912, 2/4162, 2/2370, 2/3910, 2/4291, 2/3378, 2/1532, 2/1548, 2/2984, 2/1194, 2/2024, 2/4188, 2/3141, 2/5025, 2/5026, 2/3537, 2/2021, 2/4323, 2/4416, 2/4417, 2/4418, 2/4706, 2/4911, 2/5024, 2/4292, 2/3706, 2/4650, 2/1459, 2/1545, 2/3445, 2/4529, 2/1593, 2/1794, 2/1949, 2/4814, 2/1776, 2/3536, 2/3543, 2/4891, 2/2847, 2/2664, 2/3004, 2/2023, 2/2058 ve 2/2025 esas numaralı kanun teklifleri yenilenmiştir.

Gereğini saygılarımla arz ederim.



Numan KURTULMUŞ
İstanbul Milletvekili

TBMM BAŞKANLIĞI	
Tali Komisyon	Milli Savunma Komisyonu
Esas Komisyon	Dışışleri Komisyonu
Tarih: 4.10.2023	Esas No: 2/1621

TBMM KANUNLAR ve KARARLAR BSK.LİĞİ
03 Ekim 2023
Numara

TBMM GENEL EVRAK
03 Ekim 2023
No: 1296609

TÜRKİYE BÜYÜK MİLLET MECLİSİ BAŞKANLIĞINA

Gelen Kâğıtlar Listesi'nde yayımlanan 415222 evrak numaralı "Türkiye Cumhuriyeti Hükümeti ile Macaristan Hükümeti Arasında Savunma Sanayinde Gizlilik Dereceli Bilgilerin Karşılıklı Korunmasına İlişkin Anlaşma"nın onaylanmasının uygun bulunduğu dair kanun teklifi ve gerekçesi ekte sunulmuştur.

Gereğini saygılarımla arz ederim. 18.01/2019



Binali YILDIRIM
İzmir Milletvekili
Türkiye Büyük Millet Meclisi
Başkanı

TBMM BAŞKANLIĞI		
Tali Komisyon	Milli Savunma	
Esas Komisyon	Dışişleri	
Tarih :	25 Ocak 2019	Esas No: 2/1548

TBMM
GELEN EVRAK
18 Ocak 2019
No: 416701
EBYS'ye AKTARILMIŞTIR

**TÜRKİYE CUMHURİYETİ HÜKÜMETİ İLE MACARİSTAN HÜKÜMETİ
ARASINDA SAVUNMA SANAYİNDE GİZLİLİK DERECELİ BİLGİLERİN
KARŞILIKLI KORUNMASINA İLİŞKİN ANLAŞMANIN ONAYLANMASININ
UYGUN BULUNDUĞUNA DAİR KANUN TEKLİFİ**

MADDE 1- (1) 23 Kasım 2017 tarihinde Ankara’da imzalanan “Türkiye Cumhuriyeti Hükümeti ile Macaristan Hükümeti Arasında Savunma Sanayinde Gizlilik Dereceli Bilgilerin Karşılıklı Korunmasına İlişkin Anlaşma”nın onaylanması uygun bulunmuştur.

MADDE 2- (1) Bu Kanun yayımı tarihinde yürürlüğe girer.

MADDE 3- (1) Bu Kanun hükümlerini Cumhurbaşkanı yürütür.



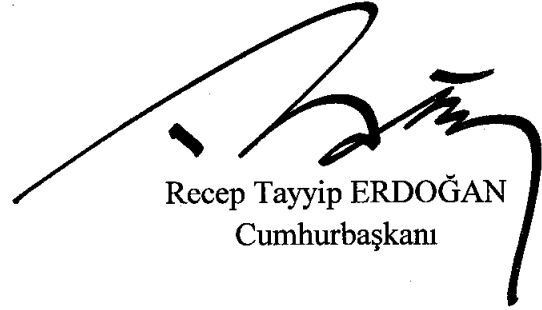
T.C. CUMHURBAŞKANLIĞI

Sayı : 68244839-599-6627
Konu : Anlaşma

15 Ocak 2019

TÜRKİYE BÜYÜK MİLLET MECLİSİ BAŞKANLIĞINA

23 Kasım 2017 tarihinde Ankara'da imzalanan "Türkiye Cumhuriyeti Hükümeti ile Macaristan Hükümeti Arasında Savunma Sanayinde Gizlilik Dereceli Bilgilerin Karşılıklı Korunmasına İlişkin Anlaşma"yı Anayasanın 90 ıncı maddesi gereğince onaylanması uygun bulunmak üzere ilişikte bilgilerinize sunarım.



Recep Tayyip ERDOĞAN
Cumhurbaşkanı

Ek:

- 1- Anlaşma (Türkçe, Macarca, İngilizce)
- 2- Genel Gerekçe

TBMM KANUNLAR ve KARARLAR BŞK.LİĞİ
15 Ocak 2019
Numara:

TBMM GELEN EVRAK
15 Ocak 2019
No: 415222
EBYS'ye AKTARILMIŞTIR

GENEL GEREKÇE

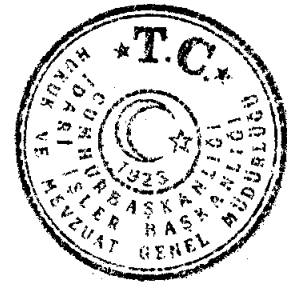
Türk savunma sanayiinin geliştirilmesi ve güçlendirilmesi ile Türk Silahlı Kuvvetlerinin modernizasyonunun sağlanması amacıyla başlatılan savunma sanayii hamlesi çerçevesinde uluslararası ilişkilerin yoğunluk kazanması ve Türkiye'deki özel sektör ağırlıklı savunma sanayii projelerine olan ilginin artması sonucunda, teknoloji transferindeki ana unsurlardan biri olan savunma sanayii güvenliği konusu büyük önem kazanmıştır.

Türkiye'nin, savunma amacıyla ihtiyaç duyduğu her türlü silah, mühimmat, araç ve gerecin doğrudan satın alma, müşterek projelere katılım, teşvik veya yatırım yolu ile tedarik edilmesi ya da bu konularda yapılacak araştırma ve geliştirme çalışmaları esnasında, savunma sanayii ile ilgili gizlilik dereceli bilgi, belge, proje ve malzemenin bilmesi gereken kişiler dışındakilere herhangi bir menfaat karşılığı veya karşılıksız olarak verilmesi ya da açıklanmasını önlemek, bunların çalınma veya sabotaja karşı korunmalarını sağlamak ülkemizin menfaatleri açısından dikkate alınması gereken önemli hususlardan biridir.

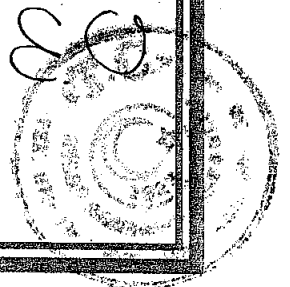
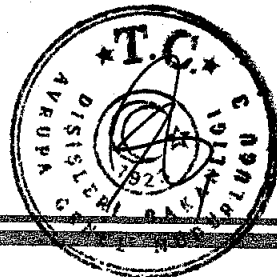
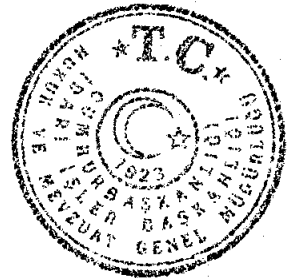
Savunma ihtiyacımız olan ve savunma sanayii ile ilgili gizlilik dereceli bilgi ihtiva eden her türlü harp silahının, mühimmatının, araç ve gereçlerinin ve bunların önemli ve kritik alt sistem ve parçalarının alımı, satımı, her tip üretim, araştırma ve geliştirme faaliyeti ile bunlara ilişkin hizmet ve altyapı tesis faaliyetlerinin tümünü kapsayan gizlilik dereceli projelerin güvenli bir şekilde yürütülmesi ve etkili bir şekilde korunması, bunlara nüfuz edecek kişilerin güvenilirliğinin sağlanması ve bunların muhafaza edileceği tesis ve yerlerin uygun şekilde emniyet altına alınması, ancak savunma sanayii güvenliğinin sağlanmasına yönelik düzenlemeler ile mümkün olabilecektir.

Bu nedenle, ülkemizde savunma sanayii güvenliğinin sağlanması, savunma sanayii güvenliği ile ilgili faaliyetlerin merkezî olarak yürütülmesi amacıyla Savunma Sanayii Millî Güvenlik Makamının belirlenmesi, ulusal menfaatlerimizin gözetilerek savunma sanayiiimizin geliştirilmesi ve güçlendirilmesini teminen 29/6/2004 tarihli ve 5202 sayılı Savunma Sanayii Güvenliği Kanunu kabul edilmiştir. Söz konusu Kanun kapsamında yer alan faaliyetler, Savunma Sanayii Millî Güvenlik Makamı olarak yetkilendirilen Millî Savunma Bakanlığının denetimi altında yürütülmektedir.

Diğer taraftan, 5202 sayılı Kanun ile Millî Savunma Bakanlığına verilen bu yetkinin uluslararası alanda kullanılabilmesi milletlerarası anlaşmalar ile mümkün olmaktadır. Bu itibarla, iki ülke arasında savunma sanayii güvenliğinin sağlanması amacıyla, ülkemizde Millî Savunma Bakanlığının denetimi altında bulunan savunma sanayii ile ilgili kamu kurum ve kuruluşları ile özel firmaları bağlayıcı nitelikte olmak üzere "Türkiye Cumhuriyeti Hükümeti ile Macaristan Hükümeti Arasında Savunma Sanayinde Gizlilik Dereceli Bilgilerin Karşılıklı Korunmasına İlişkin Anlaşma" 23 Kasım 2017 tarihinde Ankara'da imzalanmıştır.



TÜRKİYE CUMHURİYETİ HÜKÜMETİ
İLE
MACARİSTAN HÜKÜMETİ
ARASINDA
SAVUNMA SANAYİNDE
GİZLİLİK DERECELİ BİLGİLERİN KARŞILIKLI
KORUNMASINA
İLİŞKİN
ANLAŞMA



Giriş

Türkiye Cumhuriyeti Hükümeti ile Macaristan Hükümeti (bundan böyle ferdi olarak Taraf, müştereken Taraflar şeklinde anılacaktır),

Bir Tarafın ülkesinde gizlilik derecesi verilmiş ve diğer Tarafın ülkesine gönderilmiş ve/veya Taraflar ve/veya Tarafların ülkelerindeki Yetkili Kuruluşlar arasındaki karşılıklı işbirliğiyle oluşturulmuş savunma sanayine Gizlilik Dereceli Bilgilerin güvenliğini sağlamak amacıyla,

Karşılıklı koruma ve mübadeleleri ve/veya müşterek üretimleri esnasında, Taraflar ve/veya Tarafların ülkelerindeki Yetkili Kuruluşlar arasındaki savunma sanayi işbirliği çerçevesinde akdedilen Gizlilik Dereceli Sözleşmelerle ilgili Gizlilik Dereceli Bilgilerin güvenliğini sağlamaya yönelik usul ve esasların oluşturulmasına dair isteklerini belirterek,

Tarafların ulusal mevzuatlarına maruz olarak,

Bu Anlaşmanın; her iki ülkenin taraf olduğu diğer uluslararası anlaşmalardan doğan yükümlülükleri etkilemeyeceğini ve diğer devletlerin çıkarları, güvenliği ve toprak bütünlüğüne karşı kullanılmayacağını doğrulayarak,

AŞAĞIDAKİ ŞEKİLDE ANLAŞMIŞLARDIR:

MADDE 1

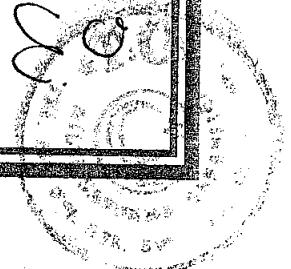
AMAÇ VE KAPSAM

İşbu Anlaşmanın amacı, kendi ilgili ulusal mevzuatına uygun olarak Tarafların ülkelerindeki Yetkili Güvenlik Makamları ve/veya Yetkili Kuruluşlar arasında gerçekleştirilen işbirliği faaliyetleri kapsamında savunma sanayiiyle ilgili Gizlilik Dereceli Bilgilerin güvenliğinin sağlanması için ilkeleri ve usulleri belirlemektir.

MADDE 2

TANIMLAR

- 1. Gizlilik Dereceli Bilgi** – her iki Tarafın ulusal mevzuatına ve bu Anlaşmaya uygun olarak, şekli, taşıyıcısı ve kayıt yöntemine bakmaksızın, yetkisiz ifşaya karşı koruma gerektiren, üretilme sürecinde olan belgeler ve malzeme dahil, savunma sanayine ilişkin her tür bilgiyi ifade eder.
- 2. Yetkili Güvenlik Makamı** – bu Anlaşmanın 3'üncü maddesinde belirtildiği şekilde, bu Anlaşmanın uygulanmasından sorumlu ve savunma sanayi veya gizlilik dereceli bilginin korunması konusunda yetkili olan Millî Makamını ifade eder.
- 3. Gizlilik Dereceli Sözleşme** – gerçekleştirilmesi Gizlilik Dereceli Bilgiye erişimi veya bu gibi bilgilerin oluşturulmasını kapsayan, özellikle, hazırlık faaliyetleri dahil olmak üzere, her tür araç ve savaş ve silah teçhizatı ile önemli ve kritik alt sistemler ve parçaların alım ve satımı, araştırma ve geliştirme ile her tür üretim, servis ve altyapı tesis ve faaliyetleri ile ilgili her tür işi kapsayan bir sözleşmeyi ifade eder.
- 4. Yüklenici** – bu Anlaşmanın hükümlerine uygun olarak Gizlilik Dereceli Sözleşmeler yapmak için hukuki ehliyete sahip, Taraflardan birinin kanunları kapsamındaki bir gerçek kişi, tüzel kişi veya başka bir teşekkülü ifade eder.



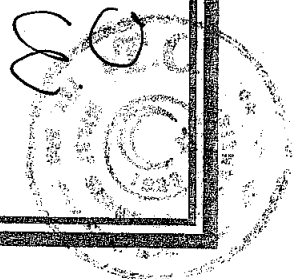
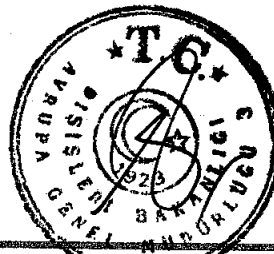
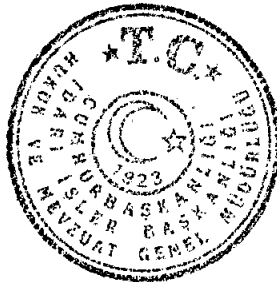
- 5. Idare** – bu Anlaşmanın hükümlerine uygun olarak Yüklenicilere Gizlilik Dereceli İhale vermek için hukuki ehliyete sahip, Taraflardan birinin kanunları kapsamındaki bir gerçek kişi, tüzel kişi veya başka bir teşekkülü ifade eder.
- 6. Tesis Güvenlik Belgesi** – bir Tarafın ulusal mevzuatına uygun olarak Yetkili Güvenlik Makamı veya başka bir yetkili kuruluş tarafından çıkarılan, Yüklenicinin Gizlilik Dereceli Bilgiyi koruma kabiliyetine sahip olduğunu doğrulayan bir belgeyi ifade eder; Yüklenici sıfatıyla hareket eden tek malikler olması durumunda Kişi Güvenlik Belgesi, Tesis Güvenlik Belgesi'nin eşiti olacaktır.
- 7. Bilmesi Gereken Prensibi** – bir kişinin resmi görevleri veya hizmetleri gerçekleştirmek için bilgilere sahip olması veya erişmesi veya bunları bilmesine ihtiyacı olduğu doğrultusunda olumlu kararın alındığı ilkeyi ifade eder.
- 8. Yetkili Kuruluşlar** – Gizlilik Dereceli Bilgiyi kendi ilgili ulusal mevzuatlarına uygun olarak kullanmaya yetkili gerçek kişiler ile hükümet kurumları, tüzel kişiler veya başka teşekküller dahil Tarafları ifade eder.
- 9. Kaynak Taraf** – kendi Tarafının ulusal mevzuatına uygun olarak Gizlilik Dereceli Bilgi çıkarma ve göndermeye yetkili Taraf, gerçek kişiler veya başka teşekkülleri ifade eder.
- 10. Alan Taraf** – kendi Tarafının ulusal mevzuatına uygun olarak Gizlilik Dereceli Bilgi almaya yetkili Taraf, gerçek kişiler veya başka teşekkülleri ifade eder.
- 11. Kişi Güvenlik Belgesi** – bir Tarafın ulusal mevzuatına uygun olarak Yetkili Güvenlik Makamı veya başka bir yetkili kuruluş tarafından çıkarılan, bir kişinin güvenlik incelemesinden geçtiğini ve Gizlilik Dereceli Bilgiye erişim için uygun olduğunu doğrulayan bir belgeyi ifade eder.
- 12. Üçüncü Taraf** – yetkisi altındaki gerçek kişi, tüzel kişi veya diğer bağlı teşekkülleri de dâhil olmak üzere bu Anlaşmaya Taraf olmayan herhangi bir ülke veya uluslararası örgüt.

MADDE 3 YETKİLİ GÜVENLİK MAKAMLARI

1. Bu Anlaşmanın uygulanmasından sorumlu olan Yetkili Güvenlik Makamları aşağıdadır:

- (1) Türkiye Cumhuriyeti için: Türkiye Cumhuriyeti Millî Savunma Bakanlığı,
Teknik Hizmetler Dairesi Başkanlığı;
- (2) Macaristan Cumhuriyeti için: Ministry for National Economy, State Secretary
Economic Development and Regulation.
Madde 8 paragraf 1, Madde 9 ve Madde 10'nun uygulamaları için Milli Güvenlik Makamı.

2. Taraflar, Paragraf 1'de bahsedilen Yetkili Güvenlik Makamlarının değişiklikleriyle ilgili olarak diplomatik kanallarla birbirlerini bilgilendireceklerdir.



MADDE 4

GÜVENLİK SINIFLANDIRMALARI

1. İlgili ulusal mevzuatlarında belirtilen güvenlik önlemleri çerçevesinde Yetkili Güvenlik Makamları ve Tarafların ülkelerindeki Yetkili Kuruluşlar, aralarında mübadele edilen veya karşılıklı işbirliğiyle üretilen Gizlilik Dereceli Bilginin korunmasını gereğince sağlamayı taahhüt ederek, aşağıdaki tabloda gösterilen Türkçe, Macarca ve İngilizce gizlilik derecesi seviyelerinin eşdeğerliğini kabul ederler:

Türkiye Cumhuriyeti'nde	Macaristan'da	İngilizce karşılığı
"ÇOK GİZLİ"	„Szigorúan titkos!"	TOP SECRET
"GİZLİ"	„Titkos!"	SECRET
"ÖZEL"	„Bizalmas!"	CONFIDENTIAL
"HİZMETE ÖZEL"	„Koriátoszt terjesztésű!"	RESTRICTED

2. Taraflardan her birinin Yetkili Güvenlik Makamı ve Yetkili Kuruluşları, diğer Tarafın Yetkili Güvenlik Makamı veya Yetkili Kuruluşlarından aldıkları Gizlilik Dereceli Bilgiyi yukarıdaki tabloya uygun olarak kendi ulusal sınıflandırma seviyesi ve İngilizce karşılığı ile işaretlemeyi taahhüt eder.

3. Tarafların Yetkili Güvenlik Makamları, güvenlik sınıflandırmalarında yapılan değişiklikler hakkında birbirlerini karşılıklı olarak bilgilendirmeyi taahhüt ederler.

4. Gizlilik Dereceli Bilgiye verilen güvenlik sınıflandırması seviyesi sadece bunlara gizlilik derecesi veren Kaynak Tarafça değiştirilebilir veya kaldırılabilir. Böyle bir değişiklik veya kaldırma kararı Kaynak Tarafça Alan Tarafa derhal bildirilecektir.

MADDE 5

GİZLİLİK DERECELİ BİLGİYİ KORUMA İLKELERİ

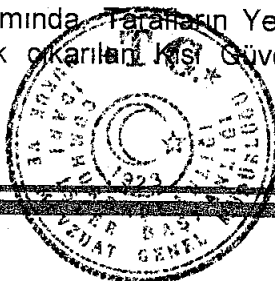
1. Taraflar, Gizlilik Dereceli Sözleşmelerin gerçekleştirilmesiyle bağlantılı olarak oluşturulan işbu belge dahil olmak üzere Taraflar arasındaki işbirliğinin sonucu olarak gönderilen veya çıkarılan Gizlilik Dereceli Bilgiyi korumak için bu Anlaşmada belirtilen ve kendi ulusal mevzuatlarına tabi her önlemi benimseyeceklerdir.

2. Yetkili Güvenlik Makamları ve/veya Tarafların ülkelerindeki Yetkili Kuruluşlar arasında karşılıklı işbirliğiyle üretilen ve/veya mübadele edilen Gizlilik Dereceli Bilgi sadece transfer amacı doğrultusunda kullanılacaktır.

3. Gizlilik Dereceli Bilgi, Kaynak Tarafın önceden yazılı onayı olmadan bir Üçüncü Tarafa ifşa edilmeyecektir.

4. Gizlilik Dereceli Bilgi sadece bilmesi gereken kişilere ve Alan Tarafın ulusal mevzuatına uygun şekilde gereğince yetkilendirilmiş kişilere ifşa edilebilir.

5. Bu Anlaşmanın kapsamında Tarafların Yetkili Güvenlik Makamları, diğer Tarafın ulusal mevzuatına uygun olarak çıkarılan Yetkili Güvenlik Belgeleri ve Tesis Güvenlik Belgelerini tanıyacaklardır.



MADDE 6

GİZLİLİK DERECELİ BİLGİNİN TRANSFERİ

1. Gizlilik Dereceli Bilgi diplomatik kanallar veya askeri ataşe yoluyla gönderilecektir.
2. HİZMETE ÖZEL / „Korlátozott terjesztésű!” / RESTRICTED olarak sınıflandırılan bilgi ayrıca Kaynak Tarafın ulusal mevzuatına uygun olarak yetkili taşıyıcılar aracılığıyla da gönderilebilir.
3. Acil durumlarda, diğer gönderim şekillerini kullanmak mümkün değilse, Kaynak Tarafın ulusal mevzuatı tarafından tanımlanan güvenlik şartlarının tanımlanması durumunda HİZMETE ÖZEL / „Korlátozott terjesztésű!” / RESTRICTED olarak sınıflandırılan bilginin yetkili kişiler tarafından kişisel olarak taşınması kabul edilebilir.
4. Tarafların Yetkili Güvenlik Makamları, kendi ilgili ulusal mevzuatlarına uygun olarak Gizlilik Dereceli Bilgiyi yetkisiz ifşaya karşı koruyan başka gönderim şekilleri üzerinde anlaşabilirler.
5. Alan Taraf, Gizlilik Dereceli Bilginin alındığını yazılı olarak doğrulayacaktır.

MADDE 7

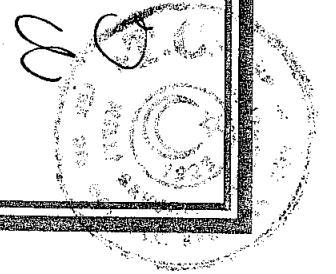
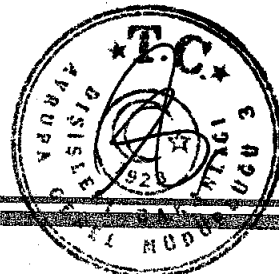
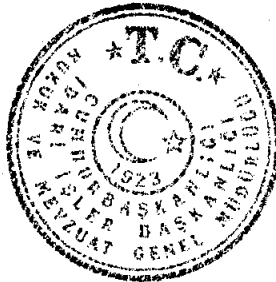
GİZLİLİK DERECELİ BİLGİLERİN TERCÜME EDİLMESİ, ÇOĞALTILMASI VE İMHA EDİLMESİ

1. ÇOK GİZLİ / GİZLİ / ÖZEL / „Szigorúan titkos!” / „Titkos!” / „Bizalmas!” / TOP SECRET / SECRET / CONFIDENTIAL güvenlik sınıflandırma seviyeleri ile işaretlenen gizlilik dereceli bilgiler sadece Kaynak Tarafın ülkesinin Yetkili Güvenlik Makamından önceden yazılı izin alınmak kaydı ile tercüme edilebilecek veya çoğaltılabilecektir.
2. Bütün tercümeler; gizlilik dereceli belgenin Kaynak Taraftan alındığını belirtecek şekilde, uygun bir güvenlik sınıflandırma işareti ve notları içerecektir. Bu şekilde tercüme edilmiş ya da çoğaltılmış belgeler orijinali ile aynı kontrol ve korumaya tâbi tutulacaktır. Nüsha ve tercümelerin sayısı, resmi amaçlar için talep edilen miktar ile sınırlı olacaktır.
3. HİZMETE ÖZEL / „Korlátozott terjesztésű!” / RESTRICTED olarak tasnif edilen bilgilerin tamamen veya kısmen birleştirilmesini engelleyecek şekilde Alan Tarafın ulusal düzenlemelerine göre imha edilecektir. Ancak; ÇOK GİZLİ / GİZLİ / ÖZEL / „Szigorúan titkos!” / „Titkos!” / „Bizalmas!” / TOP SECRET / SECRET / CONFIDENTIAL şeklinde tasnif edilen bilgiler, süresi ya da kullanım amacı sona erdiğinde imha edilmek yerine Alan Tarafça Kaynak Tarafa iade edilecektir.

MADDE 8

GİZLİLİK DERECELİ SÖZLEŞMELER

1. Gizlilik Dereceli bir Sözleşme akdedilmeden önce İdare, kendi Yetkili Güvenlik Makamından, diğer Tarafın Yetkili Güvenlik Makamının Yüklenicinin erişmesi gereken Gizlilik Dereceli Bilginin güvenlik tasnif seviyesi ile ilgili olarak geçerli bir Tesis Güvenlik Kleransına sahip olduğunun onayını almasını ister.



2. HİZMETE ÖZEL / „Korlátozott terjesztésű! / RESTRICTED olarak tasnif edilmiş olan Gizlilik Dereceli bir Sözleşme akdedilmeden önce her bir tarafın Yetkili Güvenlik Makamının, Yüklenicisinin ulusal düzenlemeler ışığında güvenlik şartlarını karşılayacağını onaylayacaktır.

3. Paragraf 1 ve 2'de bahsi geçen onaylar, Yüklenicinin, topraklarında bulunduğu tarafın ulusal düzenlemelerinde tanımlanan Gizlilik Dereceli Bilgilerin korunması bağlamındaki kriterleri karşıladığını beyan etmek için gerekli önlemlerin alındığının garantisi ile eşdeğer olacaktır.

4. Gizlilik Dereceli Bilgiler, Paragraf 1 ve 2'de bahsi geçen onaylar alınmadan Yükleniciye verilmeyecektir.

5. İdare, Gizlilik Dereceli bir Sözleşmenin uygulanmasında gerekli olan ve bu tür sözleşmelerin ayrılmaz bir parçası olarak, ÖZEL / „Bizalmas!” / CONFIDENTIAL ya da daha üstü olarak tasnif edilmiş bilgilere erişimle ilintili bir proje güvenlik talimatı yayımlayacaktır. Proje güvenlik talimatı, başlıca şu güvenlik şartlarını ihtiva etmelidir:

1) Güvenlik tasnif seviyeleri de dâhil olmak üzere, Gizlilik Dereceli Sözleşmeye ilişkin Gizlilik Dereceli Bilgi türlerinin listesi;

2) Gizlilik Dereceli Sözleşmenin uygulanması sırasında ortaya çıkan bilgilere güvenlik tasnif seviyelerinin verilmesi için gerekli kurallar.

6. İdare, Yüklenicinin Tarafının Yetkili Güvenlik Makamına ileilmek üzere kendi Tarafının Yetkili Güvenlik Makamına proje güvenlik talimatının bir kopyasını verecektir.

7. Gizlilik Dereceli bir Sözleşmenin uygulanmasında, Gizlilik Dereceli Bilgilere erişim ile ilgili kısım, Yüklenicinin, Gizlilik Dereceli Bilgilerin korunması için gerekli kriterleri proje güvenlik talimatına uygun olarak karşılaması şartıyla mümkün olacaktır.

8. Her bir altyüklenici de Yüklenici için konulan Gizlilik Dereceli Bilgilerin Korunması şartlarına aynen uymakla yükümlüdür.

9. Gizlilik Dereceli Sözleşmenin içeriğindeki Gizlilik Dereceli Bilgilere ilişkin fikri mülkiyet haklarına, ulusal düzenlemeler uygun olarak karşılıklı bir şekilde saygı duyulacaktır. Söz konusu detay ve istisnalar Gizlilik Dereceli Sözleşmelerde belirtilecektir.

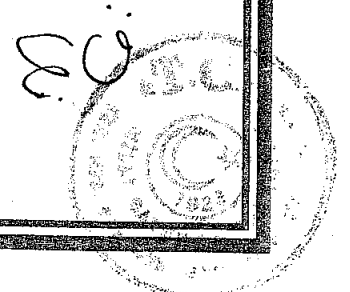
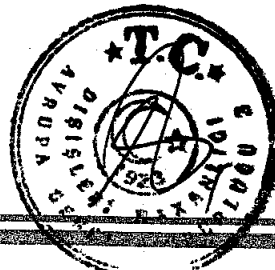
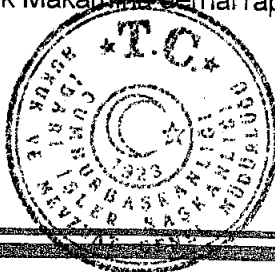
10. Bu Anlaşmanın amacı olan etkin bir işbirliği sağlayabilmek için, kendi Taraflarının ulusal mevzuatlarını kabul eden yetki kapsamında, Yetkili Güvenlik Kurulu, gerekli olması halinde, yazılı kapsamlı teknik anlaşmaları akdedebilir.

MADDE 9

GÜVENLİK İHLÂLİ

1. Güvenlik ihlali, Gizlilik Dereceli Bilgilerin korunmasına ilişkin Tarafların yasal düzenlemelerine ya da bu Anlaşmaya aykırı olarak yapılmış olan eylem ya da ihmallerdir.

2. Kaynak Tarafa ait olan veya Tarafların işbirliği sonucu ortaya çıkan Gizlilik Dereceli Bilgilere ilişkin her tür güvenlik ihlali ya da güvenlik ihlali şüphesi bilgileri, ihlalin ya da ihlal şüphesinin yer aldığı Taraf ülkenin Yetkili Güvenlik Makamına derhal rapor edilecektir.



3. Her tür güvenlik ihlali ya da güvenlik ihlali şüphesi, ortaya çıktığı Taraf ülkenin ulusal düzenlemelerine uygun olarak tahkik edilecektir.

4. Bir güvenlik ihlali halinde, ihlalin yer aldığı Taraf ülkenin Yetkili Güvenlik Makamı, diğer Tarafın Yetkili Güvenlik Makamını olay, ihlalin olduğu koşullar ve Paragraf 3'te değinilen eylemlerin sonucu hakkında yazılı olarak bilgilendirecektir.

5. Tarafların Yetkili Güvenlik Makamları, birinin diğerinden talep etmesi halinde Paragraf 3'te değinilen eylemler üzerinde işbirliği yapacaktır.

MADDE 10

ZİYARETLER

1. Tarafların Yetkili Güvenlik Makamları ve/veya ülkesindeki Yetkili Kuruluşlar arasındaki iş birliği faaliyetleri kapsamında bir Tarafın ülkesindeki Yetkili Kuruluşların tesislerine yapılacak Gizlilik Dereceli Bilgilere erişim içerikli ziyaretler, Ev Sahibi Ülkenin Yetkili Güvenlik Makamının yazılı izninin alınmasını müteakip gerçekleştirilecektir.

2. Ziyarete yönelik talepler, önerilen ziyaret tarihinden en az 21 (yirmi bir) gün öncesinden yazılı olarak Ev Sahibi ülkenin Yetkili Güvenlik Makamına bildirilecektir. Bu talepler, diplomatik kanallar ya da askeri ataşeler aracılığıyla arz edilecektir.

3. Ziyarete yönelik talep biçimleri aşağıdaki müteakip bilgileri içerecek şekilde her bir ziyaret için hazırlanacaktır.

a. Konuk personelin adı ve soyadı, doğum yeri ve tarihi, uyruğu, pasaport numarası ve görevleri

b. Öngörülen tarih, program ve tahmin edilen ziyaret süresi

c. Personel Güvenlik Kleransı düzeyi güvenlik sınıflandırma düzeyinin yanı sıra erişilecek gizlilik dereceli bilgilerin türü

d. Ziyaret edilecek yer ve tesislerin adları ve ziyaretin amacı

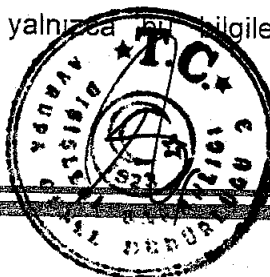
e. Konuk personeli kabul edecek kişilerin adları, soyadları ve resmi unvanları

f. Konuk personeli gönderen ülkenin Yetkili Güvenlik Makamının resmi mühürü, imzası ve istek tarihi

4. Ziyaret izni sadece belirlenen tarih ve süre için geçerli olacaktır. Ancak, işbirliğine kolaylık sağlamak amacıyla 12 ayı geçmeyen süreyi kapsayan bir ziyaret çizelgesi hazırlanabilir. Bu durumda, planlı ziyaretin izin verilen zaman süresi içerisinde sona ermeyeceği varsayıldığında bu tip ziyaretlerin süresini uzatmak gerekli olup, ziyaret talepleri Konuk Personeli gönderen ülkenin Yetkili Güvenlik Makamınca işlemdeki ziyaret izninin geçerliliğinin sona erme tarihinden en az 21 gün önce yenilenecektir.

5. 3'üncü Maddede bahsi geçen kişisel bilgileri muhafaza etmek amacıyla, Tarafların ulusal mevzuatlarına uygun olarak aşağıdaki hükümler uygulanacaktır:

a. Ev Sahibi Tarafça alınan kişisel bilgiler yalnızca bu bilgileri aktaran Tarafça tanımlanmak şart ve koşulları kullanılarak kullanılacaktır.



b. Kişisel bilgiler, amacı doğrultusunda işleme konması gerekli olduğu sürece Ev Sahibi Tarafça saklanacaktır.

c. İlgili Tarafın ulusal mevzuatlarına aykırı olarak kişisel bilgilerin aktarılması durumunda, bilgileri aktaran taraf kısmi ya da tamamen yeniden yapılandırmayı ortadan kaldıracak şekilde verilerin kaldırılmasından yükümlü olarak ev sahibi tarafı bilgilendirecektir.

d. Kişisel bilgileri aktaran taraf bu bilgilerin doğruluğundan sorumlu olacak ve bu bilgilerin eksik ya da doğru olmaması durumunda ise bilgilerin düzeltilmesi ya da çıkartılmasından yükümlü olacak olan ev sahibi tarafı bilgilendirecektir.

e. Ev sahibi Taraf ve kişisel bilgileri aktaran taraf bu bilgilerin iletilmesi, alınması ve çıkartılmasının kayıt altına alınmasından yükümlü olacaktır.

f. Kişisel bilgileri aktaran taraf ve ev sahibi taraf, işleme tabi tutulan kişisel bilgilerin yetkisiz kişilere ifşasına, yetki dışı olarak değiştirilmesine, kaybolmasına, zarar görmesine ya da tahribata uğramasına karşı etkin bir şekilde muhafazasından yükümlü olacaktır.

MADDE 11

DİLLER

Bu Anlaşmanın hükümlerinin uygulanması kapsamında, tercümenin diğer Tarafın resmi dilinde ya da İngilizce olarak eklenmesi durumunda Taraflar ya İngilizce ya da kendi resmi dilini kullanacaktır.

MADDE 12

MALİ KONULAR

Her iki Taraf da bu Anlaşmanın hükümlerinin uygulanmasından doğacak kendi masraflarını karşılayacaktır.

MADDE 13

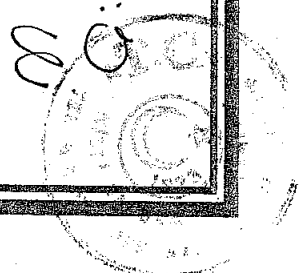
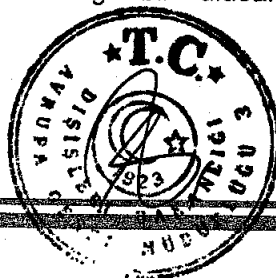
İSTİŞARE VE TADİL

1. Taraflardan biri diğer Tarafa yazılı bildirim göndererek bu Anlaşmaya istişare ve/veya tadil önerebilir.
2. Bu Anlaşma, müzakere temelinde Tarafların karşılıklı olarak yazılı onayı ile tadil edilebilir. Bahse konu tadilatlar, Madde 16'da belirtilen aynı yasal prosedürler uyarınca yürürlüğe girecektir.
3. Tarafların Yetkili Güvenlik Kuruluşları, bu Anlaşmanın uygulanmasına yönelik olarak Gizlilik Dereceli Bilgilerin Korunması kapsamında kendi yasal düzenlemelerinde yapılacak herhangi bir tadilat hususunda birbirlerine haber verecektir.

MADDE 14

UYUŞMAZLIKLARIN ÇÖZÜMÜ

1. Bu Anlaşmanın uygulanmasına yönelik herhangi bir uyuşmazlık Tarafların Yetkili Güvenlik Kuruluşları arasında yürütülecek olan doğrudan müzakerelerle çözüme kavuşturulacaktır. Uyuşmazlıklar herhangi bir çözümü, maksadı ya da herhangi bir ulusal, uluslar arası mahkemeye veya Üçüncü Tarafa intikal ettirilmeyecektir.



2. Madde 1'de bahsi geçen şekilde ihtilafa yönelik çözüm sağlanamaması halinde, uyuşmazlık diplomatik kanallarla çözümlenecektir. 45 (kırkbeş) gün içinde çözüme ulaşılamaması halinde, her iki Taraf da bu Anlaşmayı fesih edebilir.

MADDE 15

YÜRÜRLÜK SÜRESİ VE SONA ERDİRME

1. Bu Anlaşmanın yürürlük süresi 5 (beş) yıldır ve 30 (otuz) gün önceden diplomatik kanallardan sona erdirmeye talebinde bulunulmadığı sürece beş yıllık sürelerle otomatik olarak yenilenecektir.
2. Bu Anlaşmanın sona ermesi durumunda, bu Anlaşma temelinde mübadele edilen ya da oluşturulan Gizlilik Dereceli Bilgiler burada geçen hükümler uyarınca sürekli olarak korunacaktır.

MADDE 16

YÜRÜRLÜĞE GİRİŞ

1. Bu Anlaşma, Tarafların Anlaşmanın yürürlüğe girmesi için gerekli iç yasal usullerini tamamladığını birbirlerine diplomatik yollarla bildirdikleri son yazılı bildirim alındıktan 30 (otuz) gün sonra yürürlüğe girecektir.
2. Bu Anlaşma *23 Kasım 2017* tarihinde *Ankara*, 'da her biri aynı derecede geçerli olmak üzere Türkçe, Macarca ve İngilizce dillerinde ikişer asıl nüsha olarak imzalanmıştır. Bu Anlaşma hükümlerinin yorumu ile ilgili olarak herhangi bir uyuşmazlık çıkması durumunda "İngilizce metin" esas alınacaktır. İşbu Anlaşma aşağıda imzası bulunan kendi Hükümetleri tarafından yetkilendirilmiş olan temsilciler tarafından imzalanmıştır.

TÜRKİYE CUMHURİYETİ HÜKÜMETİ
ADINA

MACARİSTAN HÜKÜMETİ
ADINA

İMZA

İSİM

UNVAN : Milli Savunma Bakanı

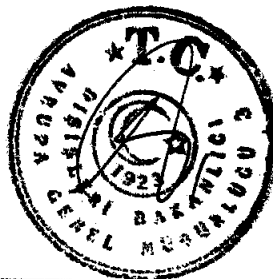
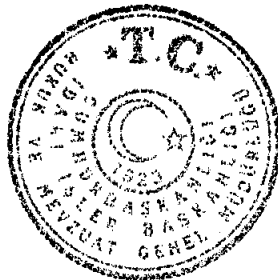
İMZA

İSİM

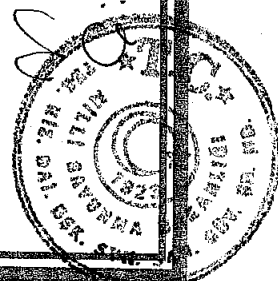
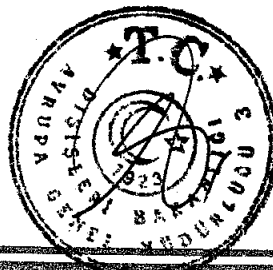
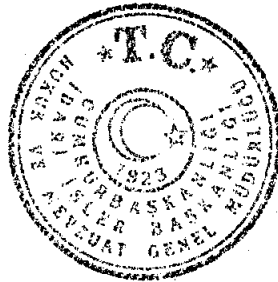
UNVAN : Dr. István Simicskó

UNVAN

: Savunma Bakanı



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

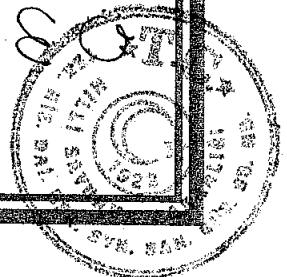
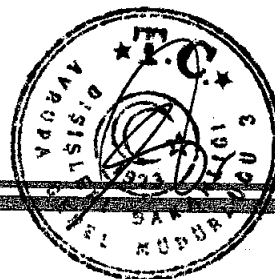
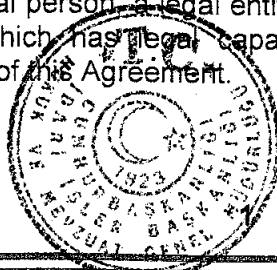
PURPOSE AND SCOPE

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

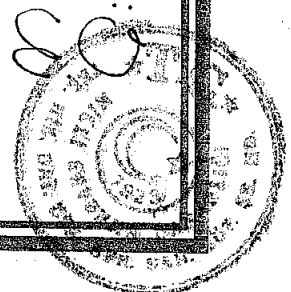
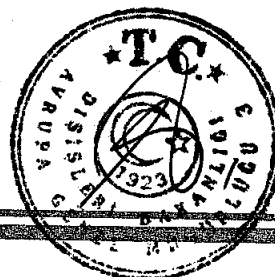
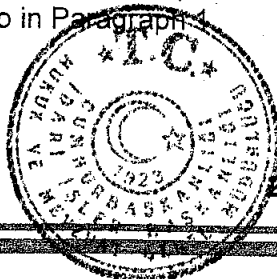
COMPETENT SECURITY AUTHORITIES

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

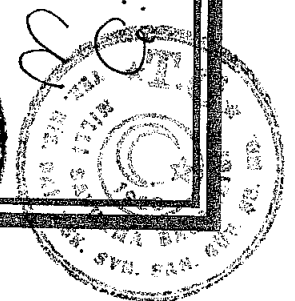
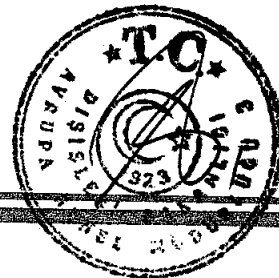
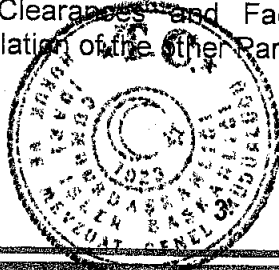
1. The Parties shall adopt every measure provided in this Agreement and subject to their national legislations in order to protect Classified Information transmitted or originated as a result of cooperation between the Parties, including this originated in connection with performance of Classified Contracts.

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

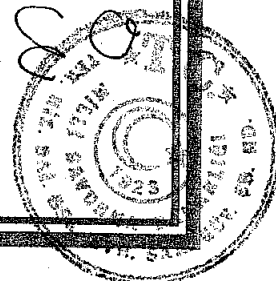
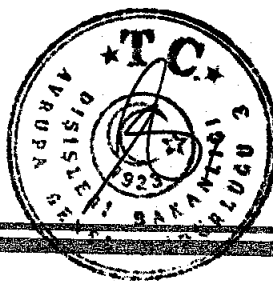
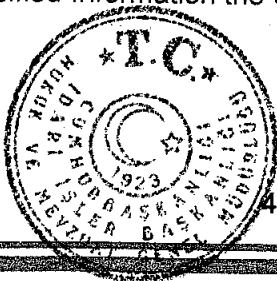
TRANSLATION, REPRODUCTION AND DESTRUCTION OF THE CLASSIFIED INFORMATION

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.

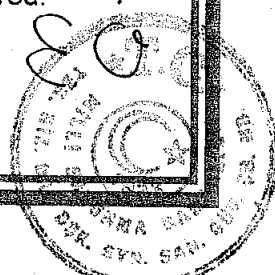
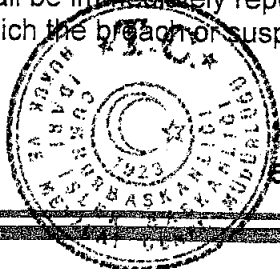
10. In order to ensure effective cooperation, which is the objective of this Agreement, and in the scope of authority acknowledged by the national legislation of their Parties, the Competent Security Authorities may, if necessary, conclude written detailed technical arrangements.

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,

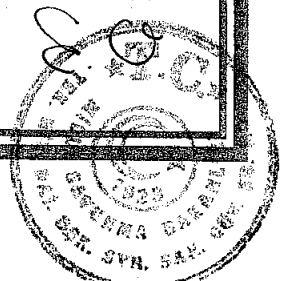
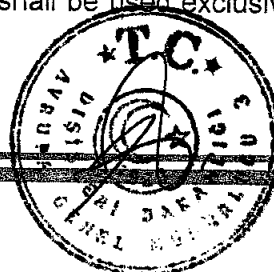
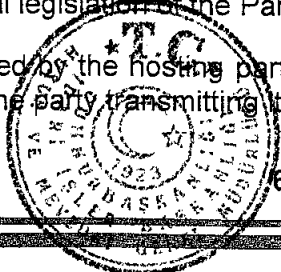
e. The names, surnames and official titles of the persons who will receive the Guest Personnel,

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

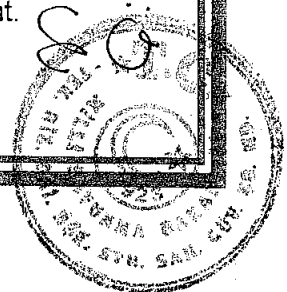
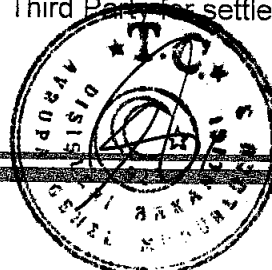
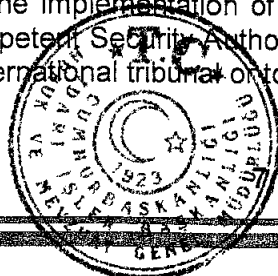
CONSULTATION AND AMENDMENT

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

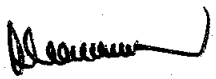
1. This Agreement is concluded for 5 (five) years and shall be then automatically renewed for five-year-periods unless terminated with 30 (thirty) days advance notice through diplomatic channels.
2. In case of termination of this Agreement, Classified Information exchanged or originated on the basis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

ARTICLE 16

ENTRY INTO FORCE

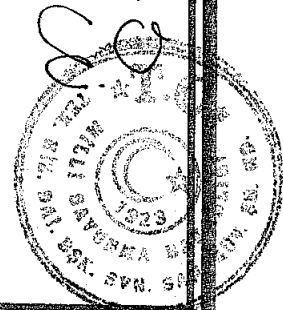
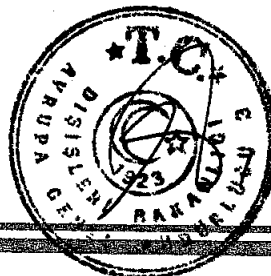
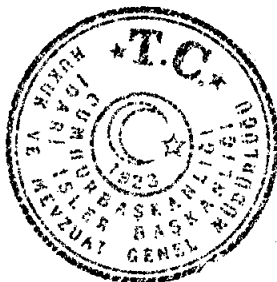
1. This Agreement shall enter into force 30 (thirty) days after the receipt of the last written notification by which the Parties notify each other, through diplomatic channels, of the completion of their internal legal procedures required for the entry into force of the Agreement.
2. This Agreement 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

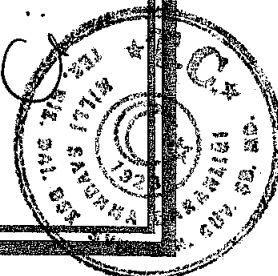
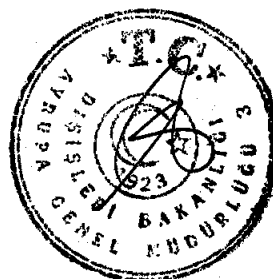
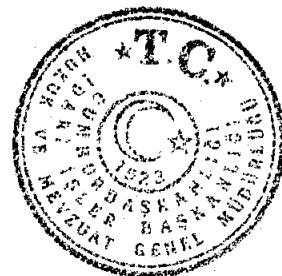
SIGNATURE : 
NAME : Nurettin CANIKLI
TITLE : Minister of National Defence

FOR THE GOVERNMENT
OF HUNGARY

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



EGYEZMÉNY
A TÖRÖK KÖZTÁRSASÁG KORMÁNYA
ÉS
MAGYARORSZÁG KORMÁNYA
KÖZÖTT
A VÉDELMI IPARI MINŐSÍTETT ADATOK
KÖLCSÖNÖS VÉDELMÉRŐL



Bevezetés

A Török Köztársaság Kormánya és Magyarország Kormánya (a továbbiakban külön a Fél, közösen a Felek),

azzal a szándékkal, hogy az általuk vagy a Felek országaiban lévő jogosult személyek által egyik Fél országában létrehozott és a másik fél országába továbbított, vagy az együttműködésük útján közösen létrehozott, védelmi ipari vonatkozású minősített adatok megfelelő védelemben részesüljenek,

kívánatosnak tartva, hogy meghatározzák azokat az eljárásokat és elveket, amelyek biztosítják a Felek és/vagy az országaikban lévő jogosult személyek védelmi ipari együttműködése keretében megkötött, minősített szerződésekkel kapcsolatos minősített adatok biztonságát a kölcsönös védelmük és cseréjük és/vagy közös létrehozásuk során,

a Felek nemzeti törvényeinek hatálya alatt, megerősítve, hogy jelen Egyezmény nem érinti az olyan egyéb nemzetközi egyezményekből származó kötelezettségeket, amelyekben egyik ország részes, és hogy ezt az egyezményt nem fogják más államok érdekei, biztonsága és területi integritása ellen felhasználni,

AZ ALÁBBIKBAN ÁLLAPODTAK MEG:

1. CIKK

CÉL ÉS ALKALMAZÁSI TERÜLET

Jelen Egyezmény célja, hogy megállapítsa azokat az eljárásokat és elveket, amelyek biztosítják a védelmi ipari minősített adatok biztonságát a Felek országaiban lévő illetékes biztonsági hatóságok és/vagy jogosult személyek együttműködése keretében, összhangban a vonatkozó nemzeti jogszabályakkal.

2. CIKK

FOGALOMMEGHATÁROZÁSOK

1. **Minősített adat:** a védelmi iparral kapcsolatos minden információ, ezen belül dokumentumok és anyagok, függetlenül azok megjelenési formájától, hordozójától és rögzítésének módjától, ideértve a létrehozás alatt állókat is, amelyek védelmet igényelnek a jogosulatlan hozzáférés ellen a jelen Egyezményben részes mindegyik ország nemzeti jogszabályai szerint.

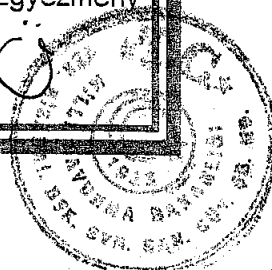
2. **Illetékes biztonsági hatóság:** az a védelmi ipari jogosultsággal vagy a minősített adatok védelmével felruházott nemzeti hatóság, amely felelős a jelen Egyezmény végrehajtásáért az alábbi 3. cikkben előírtak szerint.

3. **Minősített szerződés:** olyan szerződés, amelynek a teljesítése minősített adatokhoz való hozzáféréssel jár, vagy ilyen adatokból ered, különösen azok, amelyek bármilyen típusú katonai jármű és berendezés, ezek fontos és kritikus alrendszerei és alkatrészei beszerzésével vagy értékesítésével, kutatásával, fejlesztésével és bármiféle gyártásával, karbantartásával, infrastrukturális eszközeivel és tevékenységeivel kapcsolatos munkát érintenek, ideértve az előkészítő tevékenységeket is.

4. **Szerződő:** az egyik fél jogszabályai szerinti természetes vagy jogi személy, vagy egyéb szervezet, aki/amely jogképességgel rendelkezik a minősített szerződés jelen Egyezmény rendelkezései szerinti teljesítésére.



1



5. **Megrendelő:** az az egyik fél jogszabályai szerinti természetes vagy jogi személy, vagy egyéb szervezet, aki/amely jogképességgel rendelkezik a minősített szerződések jelen Egyezmény rendelkezései szerinti odaítélésére a szerződést kötők számára.
6. **Telephely biztonsági tanúsítvány:** az illetékes biztonsági hatóság vagy más jogosult szerv által egy Fél nemzeti jogszabályai szerint kibocsátott dokumentum, amely igazolja, hogy a Szerződő képes a minősített adatok védelmére; ha a Szerződő egyéni vállalkozó, akkor a személyi biztonsági tanúsítvány egyenértékű a telephely biztonsági tanúsítvánnyal.
7. **Szükséges ismeret elve:** az elv, amelynek megfelelően megerősítésre kerül, hogy egy személynek a hivatali feladatai vagy szolgálata ellátásához szüksége van az adathoz való hozzáférésre, annak megismerésére vagy birtoklására.
8. **Jogosult egyének:** a Felek, ezen belül a kormányzati szervek, jogi személyek vagy egyéb szervezetek, valamint a természetes személyek, amelyek/akik a vonatkozó nemzeti jogszabályokkal összhangban illetékesek a minősített adatok kezelésére.
9. **Átadó fél:** az a Fél, valamint a természetes és jogi személyek, vagy egyéb szervezetek, akik/amelyek az érintett Fél nemzeti jogszabályai szerint illetékesek a minősített adatok létrehozására és átadására.
10. **Átvevő fél:** az a Fél, valamint természetes és jogi személyek, jogi szervezetek vagy egyéb szervezetek, akik/amelyek az érintett Fél nemzeti jogszabályai szerint illetékesek a minősített adatok átvételére.
11. **Személyi biztonsági tanúsítvány:** az illetékes biztonsági hatóság vagy más jogosult szerv által egy Fél nemzeti jogszabályai szerint kibocsátott dokumentum, amely igazolja, hogy egy személy átesett a biztonsági felülvizsgálaton és alkalmas a minősített adatokhoz való hozzáférésre.
12. **Harmadik fél:** bármely olyan állam, ide értve a joghatósága alá tartozó természetes és jogi személyeket, vagy egyéb szervezeteket is, vagy nemzetközi szervezet, amely nem részese jelen Egyezménynek.

3. CIKK

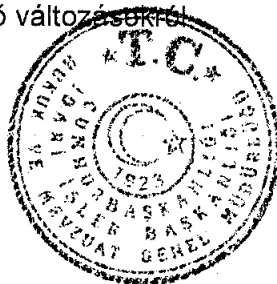
ILLETÉKES BIZTONSÁGI HATÓSÁGOK

1. A jelen Egyezmény végrehajtásáért felelős illetékes biztonsági hatóságok a következők:

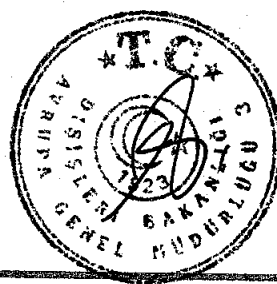
- 1) A Török Köztársaságban: A Török Köztársaság Nemzetvédelmi Minisztériuma, Műszaki Szolgáltató Főosztály
- 2) Magyarországon: Nemzetgazdasági Minisztérium, gazdaságfejlesztésért és -szabályozásért felelős államtitkár

Nemzeti Biztonsági Felügyelet a 8. Cikk 1. bekezdés, a 9. cikk és 10. cikk végrehajtása tekintetében

2. A Felek diplomáciai csatornákon tájékoztatják egymást az 1. pontban hivatkozott illetékes biztonsági hatóságokat érintő változásokról.



2



4. CIKK

MINŐSÍTÉSI SZINTEK

1. A nemzeti jogszabályaik által előírt biztonsági intézkedések keretében a Felek országaiban lévő illetékes biztonsági hatóságok és/vagy jogosult egyének kötelezettséget vállalnak, hogy megfelelően biztosítják az egymás között cserélt vagy együttműködés útján közösen létrehozott minősített adatok védelmét, és elfogadják az alábbi táblázatban török, magyar és angol nyelven bemutatott minősítési szintek megfeleltetését:

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. Mindegyik Fél illetékes biztonsági hatósága és jogosult egyénei kötelezettséget vállalnak, hogy a másik fél illetékes biztonsági hatóságától vagy jogosult egyéneitől kapott minősített adatokat ellátják a saját nemzeti minősítési szintjük jelzésével és annak angol megfelelőjével, összhangban a fenti táblázattal.

3. A Felek illetékes biztonsági hatóságai kötelezettséget vállalnak, hogy kölcsönösen tájékoztatják egymást a minősítési szintekben bekövetkezett változásokról.

4. A minősített adathoz rendelt minősítési szintet csak az átadó fél változtathatja meg, amely a minősítésüket meghatározta. Az ilyen változásról vagy megszüntetésről az átadó félnek azonnal tájékoztatnia kell az átvevő felet.

5. CIKK

A MINŐSÍTETT ADATOK VÉDELME NEK ELVEI

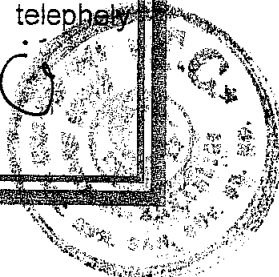
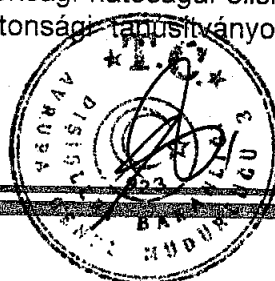
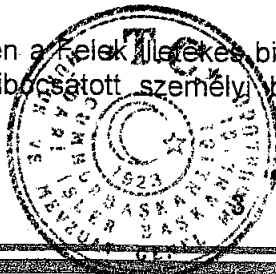
1. A Felek meghoznak minden, a jelen Egyezményben meghatározott, és nemzeti jogszabályaiknak megfelelő intézkedést, hogy megvédjék az átadott vagy együttműködésük eredményeként létrehozott minősített adatokat, ide értve azokat is, amelyek minősített szerződésekkel kapcsolatban keletkeznek.

2. A cserélt és/vagy a Felek országaiban lévő illetékes biztonsági hatóságok és/vagy jogosult egyének együttműködése keretében létrehozott minősített adatokat csak az átadás céljával összhangban használják.

3. A minősített adatokat teszik hozzáférhetővé harmadik fél részére az átadó fél előzetes írásbeli hozzájárulása nélkül.

4. A minősített adatokat csak olyan személyek részére teszik hozzáférhetővé, akik a szükséges ismeret elvének megfelelnek, és akik megfelelő jogosultsággal rendelkeznek az átvevő fél országának nemzeti jogszabályai szerint.

5. Jelen megállapodás keretében a Felek illetékes biztonsági hatóságai elismerik a másik fél nemzeti jogszabályai szerint kibocsátott személyi biztonsági tanúsítványokat és telephelyi biztonsági tanúsítványokat.



6. CIKK

A MINŐSÍTETT ADATOK ÁTADÁSA

1. A minősített adatokat diplomáciai csatornákon vagy katonai attasé útján továbbítják.
2. A HİZMETE ÖZEL / „Korlátozott terjesztésű!” / RESTRICTED minősítésű adatokat jogosult futárok útján is továbbíthatják az átadó fél nemzeti jogszabályaival összhangban.
3. Sürgős esetben, ha nincs lehetőség más továbbítási forma használatára, és teljesülnek az átadó fél nemzeti jogszabályai által előírt biztonsági követelmények, akkor megengedett a HİZMETE ÖZEL / „Korlátozott terjesztésű!” / RESTRICTED minősítésű adatok jogosult személyek által történő személyes szállítása.
4. A Felek illetékes biztonsági hatóságai megállapodhatnak a minősített adatok továbbításának olyan egyéb formáiban is, amelyek a vonatkozó nemzeti jogszabályaikkal összhangban biztosítják azok jogosulatlan hozzáférés elleni védelmét.
5. Az átvevő fél írásban igazolja a minősített adatok kézhezvételét.

7. CIKK

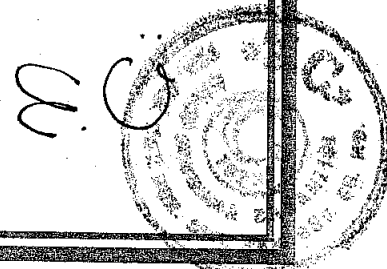
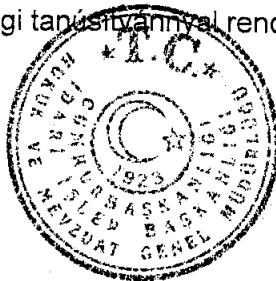
A MINŐSÍTETT ADATOK FORDÍTÁSA, MÁSOLÁSA ÉS MEGSEMMISÍTÉSE

1. A ÇOK GİZLİ / GİZLİ / ÖZEL / „Szigorúan titkos!” / „Titkos!” / „Bizalmas!” / TOP SECRET / SECRET / CONFIDENTIAL minősítésű adatok fordítására vagy másolására csak az átadó fél országa illetékes biztonsági hatóságának előzetes írásbeli hozzájárulásával kerül sor.
2. Minden fordításnak tartalmaznia kell a megfelelő biztonsági minősítés jelzését és az utalást arra, hogy a minősített dokumentumot az átadó féltől kapták. A lefordított vagy másolt minősített adatokra ugyanazok az ellenőrzési és védelmi szabályok érvényesek, mint az eredeti adatokra. A másolatok és fordítások száma nem haladhatja meg a hivatali célra szükséges mértéket.
3. A HİZMETE ÖZEL / „Korlátozott terjesztésű!” / RESTRICTED minősítésű adatokat az átvevő fél nemzeti jogszabályaival összhangban olyan módon kell megsemmisíteni, hogy a részeket ne lehessen se részlegesen, se teljesen újból összeállítani. Ettől eltérően, a ÇOK GİZLİ / GİZLİ / ÖZEL / „Szigorúan titkos!” / „Titkos!” / „Bizalmas!” / TOP SECRET / SECRET / CONFIDENTIAL minősítésű adatokat megsemmisítés helyett vissza kell juttatni az átadó félnek, amikor a minősítési idejük lejárt, vagy a felhasználási céljuk véget ért.

8. CIKK

MINŐSÍTETT SZERZŐDÉSEK

1. Minősített szerződés megkötése előtt a megrendelő kezdeményezi az illetékes biztonsági hatóságánál, hogy szerezzé be a másik Fél illetékes biztonsági hatóságától annak igazolását, hogy a szerződő a számára hozzáférhetővé váló adatok minősítési szintjének megfelelő, érvényes telephely biztonsági tanúsítvánnyal rendelkezik.



2. A HIZMETE ÖZEL / „Korlátozott terjesztésű” / RESTRICTED minősítésű adatokat érintő minősített szerződés megkötése előtt mindkét Fél illetékes biztonsági hatósága igazolja, hogy a szerződője teljesíti a nemzeti jogszabályoknak megfelelő biztonsági követelményeket.

3. Az 1. és 2. pontban hivatkozott igazolások egyenértékűek annak szavatolásával, hogy megtörténtek a szükséges intézkedések annak érdekében, hogy a szerződést kötőről ki lehessen jelenteni, hogy teljesíti annak az országnak a nemzeti jogszabályaiban a minősített adatok védelme keretében előírt kritériumokat, ahol a székhelye van.

4. Nem adhatók ki minősített adatok a szerződőnek az 1. és 2. pontban hivatkozott igazolások kézhez vétele előtt.

5. A teljesítés során ÖZEL / „Bizalmas!” / CONFIDENTIAL vagy magasabb szintű minősített adatokhoz való hozzáféréssel járó minősített szerződés megkötése előtt a megrendelő a szerződés elválaszthatatlan részét képező projekt biztonsági utasítást ad át a szerződőnek. A projekt biztonsági utasítás a biztonsági követelményekre vonatkozó előírásokat tartalmaz, különösen:

- 1) az adott minősített szerződéssel kapcsolatos minősített adatok jegyzékét, azok minősítési szintjével;
- 2) az adott minősített szerződés teljesítése során keletkező adatok biztonsági minősítési szintjének hozzárendelési szabályait.

6. A megrendelő eljuttatja a projekt biztonsági utasítás másolatát saját Fele illetékes biztonsági hatóságához, amely azt a szerződést kötő országának illetékes biztonsági hatóságához továbbítja.

7. A minősített szerződés azon részének teljesítése, amely minősített adatokhoz való hozzáféréssel kapcsolatos, azzal a feltétellel válik lehetővé, hogy a szerződő teljesíti a projekt biztonsági utasítás szerint a minősített adatok védelméhez szükséges kritériumokat.

8. Minden alvállalkozónak teljesítenie kell ugyanazokat a minősített adatok védelmére vonatkozó feltételeket, amelyeket a szerződőnek előírtak.

9. A minősített szerződés keretébe tartozó minősített adatokkal kapcsolatos szellemi tulajdonhoz fűződő jogokat kölcsönösen elismerik a nemzeti jogszabályokkal összhangban. A részleteket és a kivételeket a minősített szerződésben lehet meghatározni.

10. A jelen Egyezmény célját képező hatékony együttműködés érdekében, a Felek saját nemzeti jogszabályai által adott felhatalmazás keretei között az illetékes biztonsági hatóságok - szükség esetén - részletes, írásbeli technikai megállapodásokat köthetnek.

9. CIKK

A BIZTONSÁG MEGSÉRTÉSE

1. A biztonság megsértése: olyan tett vagy mulasztás, amely ellentétes a jelen Egyezménnyel vagy a Felek minősített adatok védelmére vonatkozó nemzeti jogszabályaival.

2. Az átadó minősített adatai vagy a Felek együttműködéséből származó minősített adatok biztonságának minden megsértéséről vagy annak gyanújáról azonnal tájékoztatják azon Fél illetékes biztonsági hatóságát, amelynek a területén a megsértés történt vagy annak gyanúja felmerült.

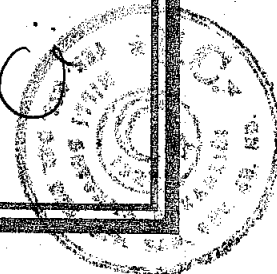
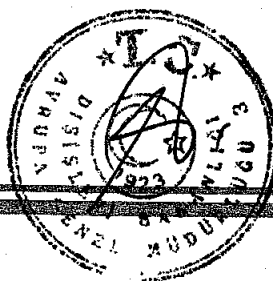


3. A biztonság minden megsértését vagy annak gyanúját azon Fél nemzeti jogszabályai szerint vizsgálják ki, amelynek a területén az előfordult.
4. A biztonság megsértése esetén azon Fél illetékes biztonsági hatósága, amelynek a területén a megsértés történt, írásban tájékoztatja a másik Fél illetékes biztonsági hatóságát a tényről, a megsértés körülményeiről és a 3. pontban hivatkozott tevékenységek kimeneteléről.
5. A 3. pontban hivatkozott tevékenységek során a Felek illetékes biztonsági hatóságai egyikük kérésére együttműködnek.

10. CIKK

LÁTOGATÁSOK

1. A Felek országaiban lévő illetékes biztonsági hatóságok és/vagy jogosult egyének együttműködési tevékenységeinek keretében az egyes Felek országaiban lévő jogosult egyének létesítményeibe tett, minősített információkhoz való hozzáféréssel járó látogatások, a fogadó ország illetékes hatóságától kapott írásbeli engedély kézhezvétele után végezhetők.
2. A látogatásra vonatkozó megkeresést a fogadó ország illetékes biztonsági hatóságához kell bejelenteni írásban, a látogatás tervezett napját legalább 21 (huszonegy) nappal megelőzően. A megkeresést diplomáciai csatornákon vagy katonai attasé útján kell benyújtani.
3. A látogatásra vonatkozó megkeresést minden egyes látogatáshoz el kell készíteni és az alábbiakat kell tartalmaznia:
 - a. A látogató vezeték- és utóneve, születési helye és ideje, állampolgársága, útlevelezs száma és beosztása,
 - b. A látogatás tervezett időpontja, programja, és várható hossza,
 - c. A személyi biztonsági tanúsítvány szintje és a hozzáférni kívánt minősített adatok típusa, valamint a biztonsági minősítés szintje,
 - d. A meglátogatandó létesítmény, helyiségek és helyek nevei és a látogatás célja,
 - e. A látogatót fogadó személyek vezeték- és keresztnévei, valamint hivatalos titulusai,
 - f. A megkeresés kelte, a látogatót küldő ország illetékes biztonsági hatóságának aláírása és hivatalos pecsétjének lenyomata.
4. A látogatási engedély csak a megadott napra vagy időszakra érvényes. Mindazonáltal, az együttműködés elősegítése érdekében összeállítható egy 12 (tizenkét) hónapot meg nem haladó látogatási ütemterv. Ebben az esetben, ha feltehető, hogy egy tervezett látogatás az engedélyezett időn belül nem fog befejeződni, és a látogatás időtartamát szükséges meghosszabbítani, akkor a látogatót küldő ország illetékes biztonsági hatóságának a látogatásra vonatkozó megkeresést meg kell újítania, legalább a folyamatban lévő látogatásra vonatkozó engedély lejártá előtt 21 (huszonegy) nappal.
5. A 3. pontban felsorolt személyi adatok védelme érdekében a következő rendelkezések alkalmazandók, a Felek nemzeti joga szerint:
 - a. A fogadó Félhez beérkezett személyi adatok kizárólag az azokat átadó Fél által meghatározott célra és feltétellel használhatók fel;



b. A fogadó Fél a személyi adatokat az azok feldolgozási céljának eléréséhez szükséges időnél tovább nem tárolhatja;

c. Ha személyi adatok az átadó Fél nemzeti jogába ütközően kerültek átadásra, akkor az átadó Fél erről a fogadó Felet köteles értesíteni, aki köteles az adatokat olyan módon törölni, hogy azok részleges vagy teljes rekonstrukcióját kiküszöbölje;

d. A személyi adatok helyességéért az azokat átadó Fél felel, és ha az adatok valótlanok vagy hiányosnak tűnnek, akkor erről köteles a fogadó Felet értesíteni, aki köteles az adatokat kijavítani vagy törölni;

e. A fogadó Fél és a személyi adatokat átadó Fél kötelesek az adatok átadását, kézhezvételét és törlését nyilvántartani;

f. A személyi adatokat átadó Fél és a fogadó fél kötelesek a feldolgozott személyi adatokat jogosulatlan személyeknek történő feltárás, az adatok jogosulatlan módosítása, sérülése és megsemmisülése ellen védeni.

11. CIKK

NYELVEK

Jelen Egyezmény rendelkezéseinek végrehajtása körében a Felek az angol nyelvet, vagy a saját hivatalos nyelvüket kötelesek használni, és az utóbbi esetben a másik Fél hivatalos nyelvére vagy angolra történő fordítást is mellékelniük kell.

12. CIKK

PÉNZÜGYI KÉRDÉSEK

Jelen Egyezmény rendelkezéseinek végrehajtásából adódó költségeiket a Felek külön-külön, saját maguk fedezik.

13. CIKK

EGYEZTETÉS ÉS MÓDOSÍTÁS

1. Bármely Fél, egy a másik Félinek címzett írásbeli értesítés küldésével javaslatot tehet egyeztetésre és/vagy a jelen Egyezmény módosítására.

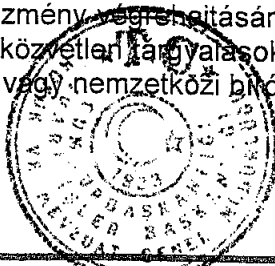
2. Jelen Egyezmény tárgyalások útján, a Felek kölcsönös írásbeli hozzájárulásával módosítható. A módosítások a 16. cikkben foglalt jogi eljárásnak megfelelően lépnek hatályba.

3. A Felek illetékes biztonsági hatóságai jelen Egyezmény végrehajtására vonatkozóan kötelesek egymást a nemzeti joguk valamennyi, a minősített adatok védelmét érintő módosításáról értesíteni.

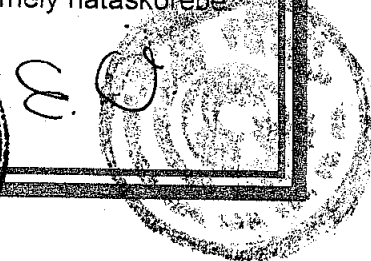
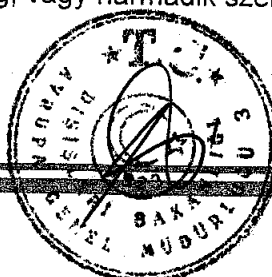
14. CIKK

VITARENDEZÉS

1. Valamennyi, a jelen Egyezmény végrehajtására vonatkozó vitát a Felek illetékes biztonsági hatóságai között lefolytatott közvetlen tárgyalások révén kell rendezni. A viták rendezése nem utalható semmilyen nemzeti vagy nemzetközi bíróságra, vagy harmadik személy hatáskörébe.



7



2. Ha valamely vita rendezése az 1. bekezdésben hivatkozott módon nem érhető el, akkor azt diplomáciai csatornákon kell rendezni. Ha a vita nem rendeződik 45 (negyvenöt) napon belül, akkor a jelen Egyezményt bármelyik Fél felmondhatja.

15. CIKK

IDŐBELI HATÁLY ÉS FELMONDÁS

1. Jelen Egyezmény 5 (öt) éves időtartamra jön létre, majd automatikusan meghosszabbítódik további 5 (öt) éves időtartamokra, kivéve ha azt diplomáciai csatornákon harminc napos felmondási idővel felmondják.

2. Jelen Egyezmény felmondása esetén a jelen Egyezmény alapján kicserélt vagy létrejött minősített adatokat továbbra is a jelen Egyezmény rendelkezéseinek megfelelően kell folytatólágosan védeni.

16. CIKK

HATÁLYBALÉPÉS

1. Jelen Egyezmény a Felek által egymásnak diplomáciai csatornákon megküldött, az Egyezmény hatálybalépéséhez szükséges belső jogi eljárásaik befejeződéséről szóló, utolsó írásbeli értesítés kézhezvétele után 30 (harminc) nappal lép hatályba.

2. Jelen Egyezményt *2017. 11. 23* -án írták alá *Ankardban* -n, török, magyar és angol nyelven, két eredeti példányban, melyek mindegyike egyaránt hiteles. A jelen Egyezmény rendelkezéseinek értelmezéséből eredő viták esetén az angol nyelvű változat irányadó.

Fentiek tanúbizonyságául az alulírott, a kormányaik által erre felhatalmazott megbízottak jelen Egyezményt aláírásukkal látták el.

A TÖRÖK KÖZTÁRSASÁG
KORMÁNYA RÉSZÉRŐL



Nurettin CANIKLI
nemzetvédelmi minisztere

MAGYARORSZÁG
KORMÁNYA RÉSZÉRŐL



Dr. Simicskó István
honvédelmi minisztere

