ACCORDO

TRA

IL GOVERNO DELLA REPUBBLICA ITALIANA

E

IL GOVERNO DELLA REPUBBLICA DI TURCHIA

SULLA RECIPROCA PROTEZIONE

DELLE INFORMAZIONI CLASSIFICATE

NELL'INDUSTRIA DELLA DIFESA

INTRODUZIONE

Il Governo della Repubblica Italiana e il Governo della Repubblica di Turchia (di seguito denominati individualmente come "la Parte" e collettivamente come "le Parti"),

Considerando gli articoli del "*Memorandum of Understanding Regarding Cooperation in the Defence Material Sector*" firmato il 15 giugno 1988,

Intendendo assicurare la sicurezza delle Informazioni Classificate relative all'industria della difesa che sono state classificate nel territorio di una Parte e trasferite nel territorio dell'altra Parte e/o generate attraverso la reciproca cooperazione tra le Parti e/o tra Enti Autorizzati negli Stati delle Parti,

Desiderando stabilire principi e procedure per garantire la sicurezza e la reciproca protezione delle Informazioni Classificate correlate ai Contratti Classificati conclusi tra le Parti e/o gli Enti Autorizzate negli Stati delle Parti nel quadro della cooperazione nell'ambito dell'industria della difesa, nonché durante lo scambio e la produzione congiunta,

Nel rispetto delle normative nazionali delle Parti,

Confermando che questo Accordo non ha effetto su diritti ed obblighi derivanti da altri accordi internazionali di cui ciascuno Stato è parte e non è utilizzato in opposizione all'interesse, alla sicurezza e all'integrità territoriale di altri Stati,

HANNO CONVENUTO QUANTO SEGUE:

ARTICOLO 1
OBIETTIVO E AMBITO

L'obiettivo del presente Accordo è stabilire principi e procedure per garantire la sicurezza delle Informazioni Classificate relative all'industria della difesa, originate e scambiate dalle Parti, dalle Competenti Autorità di Sicurezza, dagli Enti Autorizzati, da contraenti e subcontraenti, nel rispetto delle rispettive normative nazionali.

ARTICOLO 2
DEFINIZIONI

1. Informazione Classificata - qualsiasi Informazione relativa all'industria della difesa, indipendentemente dalla sua forma o natura, che richieda protezione dall'accesso non autorizzato o dall'alterazione e a cui è stato assegnato un livello di classifica di segretezza ai sensi della normativa nazionale delle Parti e del presente Accordo.

2. Autorità Competente per la Sicurezza – L'Autorità Nazionale di Sicurezza, competente ovvero debitamente autorizzata a trattare questioni relative all'industria della difesa e responsabile per l'applicazione del presente Accordo ai sensi della normativa nazionale delle Parti, come indicato nell'Articolo III del presente Accordo.

3. Contratto Classificato – un accordo tra due o più contraenti o sub-contraenti, che include o comporta l'accesso a o la creazione di Informazioni Classificate relative all'industria della difesa.

4. Contraente – una persona fisica o giuridica che, ai sensi della normativa di una delle Parti, ha la capacità giuridica di eseguire Contratti Classificati in linea con le disposizioni del presente Accordo.

5. Stazione Appaltante – una persona giuridica o altra forma di organizzazione stabilita ai sensi della normativa di una delle Parti che ha la capacità giuridica di affidare Contratti Classificati a Contraenti o Sub-contraenti in linea con le disposizioni del presente Accordo.

6. Abilitazione di Sicurezza Industriale – Un documento rilasciato dall'Autorità di Sicurezza Competente o altro ente autorizzato, in conformità con la normativa nazionale di una delle due Parti, che attesta che un Contraente ha la capacità fisica e organizzativa di trattare, conservare e proteggere Informazioni Classificate.

7. Principio della Necessità-di-Conoscere – significa la necessità di avere accesso alle Informazioni Classificate, documenti e materiali in connessione alle funzioni ufficiali e/o per lo svolgimento di un compito assegnato.

8. Enti Autorizzati – Le strutture governative, le persone giuridiche e le persone fisiche competenti per la trattazione di Informazioni Classificate ai sensi delle rispettive normative nazionali.

9. Parte Originatrice – la Parte, comprese le persone fisiche o giuridiche sottoposte alla sua giurisdizione, che origina o trasmette Informazioni Classificate.

10. Parte Ricevente – la Parte, comprese le persone fisiche o giuridiche sottoposte alla sua giurisdizione, che riceve Informazioni Classificate dalla Parte Originatrice.

11. Abilitazione di Sicurezza Personale – Un documento rilasciato ai sensi della normativa nazionale di una delle due Parti dall'Autorità di Sicurezza Competente o altra Autorità di Sicurezza Designata che conferma che un individuo è stato sottoposto ad indagine di sicurezza ed è idoneo ad avere accesso ad Informazioni Classificate.

12. Parte Terza – Ogni Stato, compreso ogni individuo, persona giuridica o altra forma di organizzazione sottoposta alla sua giurisdizione, ovvero un'organizzazione internazionale che non è parte del presente Accordo.

ARTICOLO 3
AUTORITA' DI SICUREZZA COMPETENTI

1. Le Autorità di Sicurezza Competenti responsabili per l'applicazione del presente Accordo sono:
   1) Per la Repubblica Italiana: Autorità Nazionale di Sicurezza, Dipartimento Informazioni per la Sicurezza, Ufficio Centrale per la Segretezza.
   2) Per la Repubblica di Turchia: Ministero della Difesa Nazionale della Repubblica di Turchia, Direzione Generale per i Servizi Tecnici;

2. Le Parti si informano reciprocamente tramite canali diplomatici su ogni cambiamento delle Autorità di Sicurezza Competenti indicate nel paragrafo 1, nonché su ogni emendamento alle competenze di esse.

ARTICOLO 4
CLASSIFICHE DI SEGRETEZZA

1. Nel quadro delle misure di sicurezza definite dalle rispettive normative nazionali, le Autorità di Sicurezza Competenti e gli Enti Autorizzati sotto la giurisdizione della Parti si impegnano ad assicurare debitamente la protezione delle Informazioni Classificate scambiate tra loro o generate attraverso la cooperazione reciproca, utilizzando l'equivalenza dei livelli di classifica come riportata nella tabella di seguito in lingua Italiana, Turca ed Inglese:

In Italiano	In Turco	In Inglese
SEGRETISSIMO	COK GIZLI	TOP SECRET
SEGRETO	GIZLI	SECRET
RISERVATISSIMO	ÖZEL	CONFIDENTIAL
RISERVATO	HIZMETE ÖZEL	RESTRICTED

2. Le Autorità di Sicurezza Competenti e gli Enti Autorizzati di ciascuna Parte si impegnano a contrassegnare le Informazioni Classificate che ricevono dalle Autorità di Sicurezza Competenti e dagli Enti Autorizzati dell'altra Parte con il livello equivalente di classifica di segretezza nazionale in Inglese e nella propria lingua, come indicato nella tabella di cui sopra.

3. Le Autorità di Sicurezza si informano vicendevolmente circa le rispettive legislazioni relative alle Informazioni Classificate e di ogni significativa modifica alle stesse, e si scambiano informazioni relativamente agli standard di sicurezza, alle procedure e alle pratiche per la sicurezza delle Informazioni Classificate.

4. Il livello di classifica di segretezza attribuito alle Informazioni Classificate può essere modificato o rimosso solo dalla Parte Originatrice che ha deciso tale livello. Tale decisione di modifica o rimozione è immediatamente notificata dalla Parte Originatrice alla Parte Ricevente.

ARTICOLO 5
PRINCIPI PER LA PROTEZIONE DI INFORMAZIONI CLASSIFICATE

1. Le Parti adottano ogni misura definita in questo Accordo, nel rispetto delle loro normative nazionali, al fine di proteggere le Informazioni Classificate trasmesse/scambiate ovvero originate quale risultato della cooperazione tra le Parti, inclusa la documentazione originata in connessione con l'esecuzione di Contratti Classificati.

2. Le Informazioni Classificate scambiate e/o generate attraverso la reciproca cooperazione tra le Autorità di Sicurezza Competenti e/o gli Enti Autorizzati negli Stati delle Parti sono utilizzate esclusivamente nel rispetto delle finalità del trasferimento.

3. Le Informazioni Classificate non sono disseminate a Terze Parti senza il previo consenso scritto della Parte Originatrice.

4. L'accesso e la trattazione di Informazioni Classificate possono essere consentiti solamente a persone che hanno una Necessità-di-Conoscere sulla base delle proprie funzioni e che sono state debitamente autorizzate ai sensi della normativa nazionale della Parte Ricevente.

5. Nell'ambito del presente Accordo, le Autorità di Sicurezza Competenti delle Parti riconoscono reciprocamente le Abilitazioni di Sicurezza Personali (PSC) e Industriali (FSC) rilasciate ai sensi della normativa nazionale dell'altra Parte. Le Parti cooperano inoltre garantendosi il reciproco supporto nello svolgimento delle procedure investigative e nello scambio di informazioni necessarie al rilascio delle PSC e delle FSC.

ARTICOLO 6
TRASFERIMENTO DELLE INFORMAZIONI CLASSIFICATE

1. Le Informazioni Classificate contrassegnate SEGRETISSIMO / COK GIZLI / TOP SECRET sono scambiate attraverso canali diplomatici in conformità con la normativa nazionale delle Parti. Come minimo, tali Informazioni Classificate sono trasportate sotto l'esclusivo controllo di un corriere Governativo in possesso di Abilitazione di Sicurezza al livello SEGRETISSIMO / COK GIZLI / TOP SECRET. La Parte Ricevente conferma per iscritto la ricezione delle Informazioni Classificate SEGRETISSIMO / COK GIZLI / TOP SECRET.

2. Le Informazioni Classificate fino al livello SEGRETO / GIZLI / SECRET sono trasmesse attraverso canali diplomatici o rappresentanza militare.

3. Le Informazioni Classificate RISERVATO / HIZMETE ÖZEL / RESTRICTED possono essere trasmesse anche attraverso corrieri autorizzati, nel rispetto della normativa nazionale della Parte Originatrice.

4. In casi urgenti, a meno che non sia possibile impiegare altre forme di trasmissione, se i requisiti di sicurezza definiti dalla normativa nazionale della Parte Originatrice sono rispettati, il trasporto di Informazioni Classificate RISERVATO / HIZMETE ÖZEL / RESTRICTED ad opera di individui autorizzati è consentito.

5. La Autorità di Sicurezza Competenti delle Parti possono accordarsi su altre forme di trasmissione di Informazioni Classificate che ne assicurino la protezione dalla divulgazione non autorizzata nel rispetto delle rispettive normative nazionali. La Parte Ricevente conferma per iscritto la ricezione di Informazioni Classificate.

ARTICOLO 7
TRADUZIONE, RIPRODUZIONE E DISTRUZIONE DI INFORMAZIONI CLASSIFICATE

1. Le Informazioni Classificate al livello SEGRETISSIMO / COK GIZLI / TOP SECRET, sia in forma originale che tradotte, sono tradotte o riprodotte solo previo consenso scritto dell'Autorità di Sicurezza Competente dello Stato della Parte Originatrice.

2. Tutte le traduzioni recano adeguato contrassegno di classifica di segretezza e annotazioni indicanti che il documento classificato è pervenuto dalla Parte Originatrice. Le Informazioni Classificate tradotte o riprodotte sono sottoposte allo stesso controllo e livello di protezione delle informazioni originali. Il numero di copie e traduzioni è limitato a quanto necessario per i fini ufficiali.

3. Le Informazioni Classificate sono distrutte secondo modalità che ne prevengano la ricostruzione totale o parziale.

4. Le Informazioni Classificate contrassegnate fino a SEGRETO / GIZLI / SECRET sono distrutte in conformità con la normativa nazionale delle Parti.

5. Le Informazioni Classificate contrassegnate SEGRETISSIMO / COK GIZLI / TOP SECRET non possono essere distrutte. Esse sono restituite all'Autorità di Sicurezza Competente della Parte Originatrice.

6. Un rapporto relativo alla distruzione di Informazioni Classificate è compilato e trasmesso all'Autorità di Sicurezza della Parte Originatrice, unitamente alla sua traduzione in Inglese.

7. In caso di situazione di crisi in cui sia impossibile proteggere o restituire Informazioni Classificate, queste sono distrutte immediatamente. La Parte Ricevente informa l'Autorità di sicurezza della Parte Originatrice circa la distruzione appena possibile.

ARTICOLO 8
CONTRATTI CLASSIFICATI

1. Prima di concludere un Contratto Classificato, la Stazione Appaltante chiede alla sua Autorità Competente per la Sicurezza di ricevere conferma dall'Autorità Competente per la Sicurezza dell'altra Parte che il Contraente sia in possesso di un'Abilitazione di Sicurezza Industriale corrispondente al livello di Classifica delle Informazioni Classificate cui il Contraente avrà accesso.

2. Prima di concludere un Contratto Classificato relativo a Informazioni Classificate al livello RISERVATO / HIZMETE ÖZEL / RESTRICTED, l'Autorità Competente per la Sicurezza di ciascuna Parte conferma che il proprio Contraente rispetta i requisiti di sicurezza previsti dalla legislazione nazionale.

3. La conferma di cui ai Paragrafi 1 e 2 equivale alla garanzia che sono state svolte le azioni necessarie al fine di dichiarare che il Contraente rispetti i criteri in materia di protezione delle Informazioni Classificate previsti dalla normativa nazionale della Parte nel cui territorio è stabilito.

4. Le Informazioni Classificate non sono rilasciate al Contraente prima di ricevere la conferma di cui ai Paragrafi 1 e 2.

5. La Stazione Appaltante pubblica le istruzioni di sicurezza del progetto (PSI) necessarie a svolgere il Contratto Classificato relativo alle Informazioni Classificate al livello RISERVATISSIMO / ÖZEL / CONFIDENTIAL o superiore, che è parte integrante di tale Contratto Classificato. Le istruzioni di sicurezza del progetto contengono disposizioni relative ai requisiti di sicurezza, con particolare riferimento a:

a) La tipologia di Informazioni Classificate correlate al Contratto Classificato, inclusi i relativi livelli di classifica di segretezza;
b) I criteri sulla base dei quali i livelli di classifica sono attribuiti alle informazioni originate nell'esecuzione del Contratto Classificato.

6. La Stazione Appaltante invia una copia delle istruzioni di sicurezza del progetto all'Autorità Competente per la Sicurezza della sua Parte, che la trasmette all'Autorità di Sicurezza Competente del Contraente per approvazione.

7. L'accesso ad Informazioni Classificate nell'ambito dell'esecuzione del Contratto Classificato è possibile a condizione che il Contraente rispetti i criteri necessari per la protezione di Informazioni Classificate, in linea con quanto stabilito nelle istruzioni di sicurezza del progetto.

8. Ogni subcontraente si conforma agli stessi requisiti di protezione delle Informazioni Classificate previste per il Contraente,

9. I diritti di proprietà intellettuale riguardanti le Informazioni Classificate prodotte nell'ambito del Contratto Classificato sono rispettati reciprocamente nel rispetto delle normative nazionali. Gli aspetti di dettaglio e le eccezioni possono essere specificate all'interno del Contratto Classificato.

ARTICOLO 9
VIOLAZIONI DI SICUREZZA

1. Una Violazione di Sicurezza è un'azione o un'omissione contraria al presente Accordo, ovvero alla normativa nazionale delle Parti in materia di protezione delle Informazioni Classificate.

2. Informazioni su ogni sospetta o effettiva Violazione di Sicurezza relativa ad Informazioni Classificate originate da una delle Parti ovvero come risultato della cooperazione tra le Parti sono immediatamente trasmesse all'Autorità Competente per la Sicurezza della Parte nel cui territorio è avvenuta la violazione o presunta violazione.

3. Ogni Violazione di Sicurezza effettiva o sostanziale è oggetto di investigazione ai sensi della normativa nazionale della Parte nel cui territorio è avvenuta.

4. In caso di Violazione di Sicurezza l'Autorità Competente per la Sicurezza della Parte nel cui territorio è avvenuta la Violazione informa l'Autorità Competente per la Sicurezza dell'altra Parte per iscritto in relazione al fatto accaduto, alle circostanze della Violazione e al risultato delle azioni di cui al Paragrafo 3.

5. Le Autorità Competenti per la Sicurezza delle Parti cooperano nello svolgimento delle azioni di cui al Paragrafo 3, su richiesta di una di esse.

ARTICOLO 10
VISITE

1. Le Visite alle strutture degli Enti Autorizzati nello Stato di ciascuna Parte che comportano l'accesso ad Informazioni Classificate nell'ambito delle attività di cooperazione tra le Autorità Competenti per la Sicurezza e/o Enti Autorizzati negli Stati delle Parti sono svolte previa ricezione dell'autorizzazione scritta dell'Autorità Competente per la Sicurezza del Paese ospitante.

2. Le richieste di visita sono notificate all'Autorità Competente per la Sicurezza del Paese ospitante per iscritto, non più tardi di 21 (ventuno) giorni prima della data di visita proposta. Tali richieste sono trasmesse attraverso canali diplomatici o rappresentanza militare.

3. Il modulo di richiesta predisposto per ciascuna Visita include le seguenti Informazioni:
   a. Nome, cognome, data e luogo di nascita, nazionalità, numero di passaporto e funzione del personale ospite,
   b. La data proposta, il programma e la durata della visita,
   c. Il livello di Abilitazione di Sicurezza, la tipologia ed il livello delle Informazioni Classificate cui è previsto l'accesso,
   d. La denominazione degli edifici, delle strutture e dei luoghi oggetto di visita, unitamente alle finalità della stessa,

e. I nomi, cognomi e le funzioni ufficiali delle persone che riceveranno il personale ospite,
f. Le date di richiesta, firma, e timbro ufficiale dell'Autorità Competente del Paese che invia il personale ospite.

4. Un permesso di visita ha validità unicamente per le date o per il periodo indicato. Tuttavia, al fine di facilitare la cooperazione, può essere predisposto un programma di visita relativo ad un periodo non superiore a 12 (dodici) mesi. In tal caso, laddove una visita già pianificata non si concluda nelle tempistiche concordate e sia necessario estendere la durata della stessa, la richiesta di visita è rinnovata dall'Autorità Competente per la Sicurezza della Parte che invia il personale ospite, almeno 21 (ventuno) giorni prima della scadenza della validità dell'autorizzazione alla visita in corso.

5. Al fine di proteggere i dati personali di cui al Paragrafo 3, si applicano le seguenti disposizioni, nel rispetto della normativa nazionale delle Parti:

a. I dati personali ricevuti dalla parte ospitante sono impiegati esclusivamente per le finalità e alle condizioni definite dalla Parte che le trasmette;
b. I dati personali sono custoditi dalla parte ospitante solo al fine di e per il periodo necessario a raggiungere lo scopo per il quale sono detenuti;
c. Nel caso in cui i dati personali siano trasmessi in violazione della normativa nazionale di una Parte, la Parte che li ha trasmessi informa la Parte ospitante, che è tenuta alla cancellazione dei dati in modo da renderne impossibile la ricostruzione totale o parziale;
d. La Parte che trasmette i dati personali è responsabile per la correttezza degli stessi. Nel caso in cui i dati risultino errati o incompleti, l'altra parte è informata ai fini della correzione o rimozione degli stessi.
e. Le parti tengono nota della trasmissione, della registrazione e della cancellazione dei dati.

ARTICOLO 11
LINGUE

1. Nell'ambito applicativo delle disposizioni del presente Accordo, le Parti utilizzano l'Inglese o le loro lingue ufficiali. In tale, secondo caso, la traduzione nella lingua ufficiale dell'altra Parte ovvero in Inglese è annessa.

2. In caso di interpretazioni confliggenti, l'interpretazione del testo in Inglese prevale.

ARTICOLO 12
ASPETTI FINANZIARI

1. L'attuazione del presente Accordo non comporta, in principio, alcun costo.

2. Nel rispetto del Paragrafo 1, ciascuna Parte si fa carico di eventuali costi non previsti connessi all'attuazione del presente Accordo.

ARTICOLO 13
CONSULTAZIONE ED EMENDAMENTO

1. Ciascuna Parte può proporre la consultazione e/o l'emendamento del presente Accordo mediante notifica scritta trasmessa all'altra Parte attraverso canali diplomatici.

2. Il presente Accordo può essere emendato tramite reciproco consenso scritto delle Parti all'esito di una negoziazione Gli emendamenti entrano in vigore con la stessa procedura prevista dall'Articolo 17.

3. Le Autorità Competenti per la Sicurezza delle Parti si informano reciprocamente di qualsiasi modifica alla legislazione nazionale sulla protezione delle Informazioni Classificate che abbia impatto sull'applicazione del presente Accordo.

4. Al fine di assicurare l'efficace cooperazione oggetto del presente Accordo e nell'ambito delle funzioni ad esse conferite dalla normativa nazionale delle Parti, le Autorità Competenti per la Sicurezza possono, ove necessario, concludere intese attuative di dettaglio.

ARTICOLO 14
SOLUZIONE DELLE CONTROVERSIE

1. Qualsiasi controversia riguardante l'attuazione del presente Accordo è risolta attraverso la negoziazione diretta tra le Autorità Competenti per la Sicurezza delle Parti. Le controversie non sono deferite ad alcun tribunale nazionale o internazionale, né a terze Parti per la soluzione.

2. Laddove non si pervenga alla soluzione di una controversia nei termini descritti dal Paragrafo 1, tale disputa è risolta attraverso la negoziazione per il tramite di canali diplomatici. Se non si perviene ad una soluzione entro 45 (quarantacinque) giorni lavorativi dalla ricezione della notifica scritta, ciascuna Parte può porre fine al presente Accordo.

3. Nelle more della conclusione delle procedure negoziali, sia in via diretta che per canali diplomatici, le Parti continuano ad applicare le disposizioni del presente Accordo.

ARTICOLO 15
NORMATIVA APPLICABILE

Il presente Accordo è attuato nel rispetto della normativa nazionale di entrambe le Parti, degli Accordi internazionali di cui esse sono parte e degli obblighi derivanti dalla loro appartenenza ad organizzazioni internazionali, unioni ed entità regionali e sub-regionali.

ARTICOLO 16
EFFICACIA TEMPORALE E DENUNCIA

1. Il presente Accordo è concluso per un periodo di tempo di 5 (cinque anni) ed è rinnovato automaticamente per i successivi cinque anni, a meno di formale notifica di una Parte all'altra, per iscritto e tramite canali diplomatici, 30 (trenta) giorni prima della cessazione dell'Accordo, dell'intenzione di denunciare l'Accordo.

2. Ciascuna parte può porre fine al presente Accordo in qualsiasi momento dando previa comunicazione scritta in tale senso all'altra Parte tramite canali diplomatici. In tal caso, il presente Accordo cessa di produrre effetti dopo 3 (tre) giorni dalla data di ricezione della notifica. In caso di cessazione del presente Accordo, le Informazioni Classificate scambiate o originate sulla base dello stesso continuano ad essere protette in linea con le disposizioni in esso contenute.

3. In caso di controversia, se non si raggiunge una soluzione, ciascuna Parte può risolvere il presente Accordo.

ARTICOLO 17
ENTRATA IN VIGORE

Il presente Accordo entra in vigore alla data di ricezione dell'ultima comunicazione scritta con cui le Parti si informano a vicenda, per il tramite di canali diplomatici, del completamento delle rispettive procedure legislative interne per l'entrata in vigore dello stesso.

ARTICOLO 18
TESTO E FIRMA

1. Fatto ad Ankara il 5 luglio 2022 in due originali ciascuno in lingua italiana, turca e inglese, tutti i testi facendo ugualmente fede. In caso di divergenze interpretative, il testo in lingua inglese prevale.

2. In fede che i sottoscritti, debitamente autorizzati, hanno firmato il presente Accordo.

PER IL GOVERNO
DELLA REPUBBLICA ITALIANA

FIRMA:

NOME:

CARICA:

PER IL GOVERNO
DELLA REPUBBLICA DI TURCHIA

FIRMA:

NOME:

CARICA:

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

GİRİŞ

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

15 Haziran 1988 tarihinde imzalanan "Savunma Malzemeleri Sektöründe İşbirliği Yapılmasına Dair Mutabakat Muhtırası"nın hükümleri göz önünde bulundurularak,

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

Taraflar ve/veya tarafların ülkelerindeki Yetkili Kuruluşlar arasında imzalanan savunma sanayi işbirliği çerçevesinde akdedilen Gizlilik Dereceli Sözleşmelerle ilgili Gizlilik Dereceli Bilginin paylaşımı ve/veya ortak üretimi kapsamında güvenliğini karşılıklı olarak korunmasını sağlamaya yönelik ilke ve usullerin belirlenmesine dair isteklerini belirterek,

Tarafların kendi yasal mevzuatlarına tabi olmak üzere,

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

AŞAĞIDA BELİRTİLDİĞİ ÜZERE ANLAŞMIŞLARDIR:

MADDE 1
AMAÇ VE KAPSAM

İşbu Anlaşmanın amacı, Tarafların kendi ilgili ulusal mevzuatına uygun olarak ülkelerindeki Yetkili Güvenlik Makamları, Yetkili Kuruluşlar, yükleniciler ve alt yükleniciler arasında gerçekleştirilen işbirliği faaliyetleri kapsamında savunma sanayiyle ilgili Gizlilik Dereceli Bilginin güvenliğini sağlayacak ilke ve usulleri belirlemektir.

MADDE 2
TANIMLAR

İşbu Anlaşma kapsamında:

1. Gizlilik Dereceli Bilgi- Tarafların ulusal mevzuatına ve işbu Anlaşmaya uygun olarak, şekli, taşıyıcısı ve kayıt yöntemine bakılmaksızın, yetkisiz erişime, tahrife karşı koruma gerektiren ve gizlilik derecesi verilen savunma sanayine ilişkin her tür bilgiyi ifade eder.

2. Yetkili Güvenlik Makamı- İşbu Anlaşmanın 3. maddesinde belirtilen, Tarafların ulusal mevzuatı uyarınca savunma sanayii konuları ile ilgilenmeye yetkili ya da tam yetkili ve işbu Anlaşmanın uygulanmasından sorumlu Milli Güvenlik Makamını ifade eder.

3. Gizlilik Dereceli Sözleşme- Gizlilik Dereceli Bilginin, savunma sanayii ile ilgili gerçekleştirilecek olan faaliyetlere dair bilgiye erişimi kapsayan ve iki veya daha fazla yüklenici ya da alt yüklenici arasında imzalanan sözleşmeyi ifade eder.

4. Yüklenici- İşbu Anlaşma metni hükümlerine uygun olarak Gizlilik Dereceli Sözleşmeler yapma hukuki ehliyetine sahip ve ilgili tarafın hukuki mevzuatı kapsamındaki gerçek ve tüzel kişileri ifade eder.

5. İhale Makamı- İşbu Anlaşma hükümlerine uygun olarak Yüklenici veya Alt Yükleniciler ile Gizlilik Dereceli Sözleşmeler yapmak için yasal yetkiye sahip ve Taraflardan birinin kanunları kapsamında yer alan tüzel kişi veya diğer teşekkülleri ifade eder.

6. Tesis Güvenlik Belgesi- Bir Tarafın ulusal mevzuatına uygun olarak Yetkili Güvenlik Makamı veya bir diğer yetkili kuruluşu tarafından çıkarılan ve Yüklenicinin Gizlilik Dereceli Bilgiyi fiziki ve kurumsal olarak tutma, depolama ve koruma kabiliyetine sahip olduğunu doğrulayan belgeyi ifade eder.

7. Bilmesi Gereken Prensibi- Resmi Görev ile ilgili olarak ve/veya somut bir görevin yerine getirilmesine yönelik Gizlilik Dereceli Bilgi, Belge ve Malzemeye erişim gereğini ifade eder.

8. Yetkili Kuruluşlar- İlgili Tarafların ulusal mevzuatları uyarınca Gizlilik Dereceli Bilgiyi idare etme yetkisini haiz devlet kurumları ile gerçek ve tüzel kişileri ifade eder.

9. Kaynak Taraf- Gizlilik Dereceli Bilgiyi oluşturan ya da Alan Tarafa transfer eden Tarafça yetkilendirilmiş tüzel ve gerçek kişileri ifade eder.

10. Alan Taraf- Gizlilik Dereceli Bilgiyi almaya yetkili Tarafca yetkilendirilmiş tüzel ve gerçek kişileri ifade eder.

11. Kişi Güvenlik Belgesi- Taraflardan birinin ulusal mevzuatına uygun olarak, Yetkili Güvenlik Makamı ya da diğer Yetkilendirilmiş Güvenlik Kuruluşu tarafından verilen, kişinin güvenlik incelemesinden geçtiğini ve Gizlilik Dereceli Bilgiye erişime uygun olduğunu doğrulayan belgeyi ifade eder.

12. Üçüncü Taraf- İşbu Anlaşmaya Taraf olmayan ve kendi mevzuatına tabi gerçek ve tüzel kişilikleri ve/veya diğer teşekkülleri kapsayan ülke veya uluslararası örgütleri ifade eder.

MADDE 3
YETKİLİ GÜVENLİK MAKAMLARI

1. Bu Anlaşmanın uygulanmasından sorumlu olan Yetkili Güvenlik Makamları aşağıdadır:
   1) İtalya Cumhuriyeti adına: Ulusal Güvenlik Dairesi, Güvenlik ve Enformasyon Başkanlığı – Merkezi Gizlilik Şubesi
   2) Türkiye Cumhuriyeti adına: Türkiye Cumhuriyeti Millî Savunma Bakanlığı, Teknik Hizmetler Genel Müdürlüğü;

2. Taraflar, 1. Fıkra'da bahsi geçen Yetkili Güvenlik Makamlarında veya yetkilerinde yapılacak olan değişiklikler hakkında birbirlerini diplomatik kanallarla bilgilendireceklerdir.

MADDE 4
GİZLİLİK DERECELERİ

1. İlgili Tarafların 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 sağlamayı taahhüt ve aşağıdaki tabloda gösterilen İtalyanca, Türkçe ve İngilizce gizlilik derecelerinin eşdeğerliğini kabul ederler:

İtalyanca	Türkçe	İngilizce
"SEGRETISSIMO"	"ÇOK GİZLİ"	"TOP SECRET"
"SEGRETO"	"GİZLİ"	"SECRET"
"RISERVATISSMO"	"ÖZEL"	"CONFIDENTIAL"
"RISERVATO"	"HİZMETE ÖZEL"	"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, kendi mevzuatlarında belirtilen güvenlik sınıflandırmaları ve bu sınıflandırmalar üzerinde yapılacak değişiklikler ile Gizlilik Dereceli Bilgiyi korurken kullandıkları kendi güvenlik standartları, usulleri ve uygulamaları hakkında birbirlerini karşılıklı olarak bilgilendirmeyi taahhüt ederler.

4. Gizlilik Dereceli Bilgiye verilen güvenlik seviyesi sadece gizlilik derecesini veren Kaynak Tarafça değiştirilebilir veya kaldırılabilir. Değişiklik veya kaldırma kararları Kaynak Tarafça Alan Tarafa derhal bildirilecektir.

MADDE 5
GİZLİLİK DERECELİ BİLGİYİ KORUMA İLKELERİ

1. Gizlilik Dereceli Sözleşmelerin uygulanması ile ilgili olarak oluşturulan bu belge de dâhil, Taraflar aralarındaki işbirliği neticesinde transfer/mübadele edilen veya oluşturulan Gizlilik Dereceli Bilgiyi korumak için işbu Anlaşmada öngörülen ve kendi ulusal mevzuatlarına tabi olan bütün önlemleri alacaktır.

2. Yetkili Güvenlik Makamları ve/veya Tarafların ülkelerindeki Yetkili Kuruluşlar arasında karşılıklı işbirliğiyle üretilen ve/veya mübadele edilen Gizlilik Dereceli Bilgi yalnızca transfer amacıyla kullanılabilecektir.

3. Gizlilik Dereceli Bilgi, Kaynak Tarafın yazılı onayı alınmadan Üçüncü Tarafa ifşa edilmeyecektir.

4. Gizlilik Dereceli Bilgiye, yalnızca bilmesi gereken kişiler ve Alan Tarafın ulusal mevzuatına uygun şekilde yetkilendirdiği kişiler erişilebilir ve kullanılabilir.

5. İşbu Anlaşma kapsamında, Tarafların Yetkili Güvenlik Makamları diğer Tarafın kendi ulusal mevzuatı çerçevesinde vereceği Kişi Güvenlik Belgeleri (KGB) ile Tesis Güvenlik Belgelerini (TGB) karşılıklı olarak tanıyacaklardır. Taraflar KGB'leri ile TGB'lerinin verilebilmesi için gereken güvenlik incelemesi usullerini ve bilgi değişiminde müştereken çalışacak ve birbirlerini karşılıklı olarak destekleyeceklerdir.

MADDE 6
GİZLİLİK DERECELİ BİLGİNİN TRANSFERİ

1. ÇOK GİZLİ / SEGRETISSIMO / TOP SECRET gizlilik derecesine haiz bilgi, Taraflar arasında kendi ulusal mevzuatlarına uygun olarak diplomatik kanallar aracılığı ile gönderilecektir. Söz konusu gizlilik derecesine haiz bilgiyi taşıyacak Hükümet kuryesi en az ÇOK GİZLİ / SEGRETISSIMO / TOP SECRET seviyesinde Kişi Güvenlik Belgesine sahip olmalıdır. Alan Taraf, ÇOK GİZLİ / SEGRETISSIMO / TOP SECRET Gizlilik Dereceli Bilginin alındığını yazılı olarak doğrulamakla mükelleftir.

2. GİZLİ / SEGRETO / SECRET gizlilik derecesine kadar gizlilik derecesine haiz bilgi diplomatik kanallar ya da askeri ataşe aracılığı ile gönderilebilecektir.

3. HİZMETE ÖZEL / RISERVATO / RESTRICTED gizlilik derecesine haiz bilgi Kaynak Tarafın ulusal mevzuatına uygun olarak yetkilendirdiği kuryeler aracılığıyla da gönderilebilir.

4. Acil durumlarda, başka gönderim yöntemleri kullanmanın mümkün olmadığı durumlarda, Kaynak Tarafın ulusal mevzuatınca belirlenen güvenlik şartlarının karşılanması koşulu ile HİZMETE ÖZEL / RISERVATO / RESTRICTED olarak sınıflandırılan bilginin yetkili kişiler tarafından taşınması kabul edilebilir.

5. Tarafların Yetkili Güvenlik Makamları, kendi ilgili ulusal mevzuatlarına uygun olarak Gizlilik Dereceli Bilgiyi yetkisiz ifşaya karşı koruyan başka gönderim yöntemleri üzerinde de anlaşabilirler. Alan Taraf, Gizlilik Dereceli Bilginin alındığını yazılı olarak doğrulamakla mükelleftir.

MADDE 7
GİZLİLİK DERECELİ BİLGİLERİN TERCÜME EDİLMESİ, ÇOĞALTILMASI VE İMHA EDİLMESİ

1. ÇOK GİZLİ / SEGRETISSIMO / TOP SECRET güvenlik derecesindeki, orijinal nüsha ve tercümeye ait, Gizlilik Dereceli Bilgiler sadece Kaynak Tarafın ülkesinin Yetkili Güvenlik Makamından önceden yazılı izin alınmak kaydı ile tercüme edilebilecek veya çoğaltılabilecektir.

2. Bütün tercümelerde gizlilik dereceli belgenin Kaynak Taraftan alındığını belirtilecek ve uygun güvenlik derecesi belirtilecek ve açıklama notlarını içerecektir. Tercüme edilmiş ya da çoğaltılmış Gizlilik Dereceli Bilgi orijinal bilgi ile aynı kontrol ve koruma mekanizmalarına tâbi tutulacaktır. Nüsha ve tercümelerin sayısı, resmi amaçlar için talep edilen miktar ile sınırlı olacaktır.

3. Gizlilik Dereceli Bilgi kısmi ya da tam olarak yeniden birleştirilmesine izin verilmeyecek şekilde imha edilecektir.

4. GİZLİ / SEGRETO / SECRET gizlilik derecesine kadar sınıflandırılmış olan Gizli Bilgi, Tarafların kendi mevzuatları çerçevesinde imha edilecektir.

5. ÇOK GİZLİ / SEGRETISSIMO / TOP SECRET gizlilik derecesine haiz Gizli Bilgi imha edilmeyecek, Kaynak Tarafın Yetkili Güvenlik Makamına iade edilecektir.

6. Gizlilik Dereceli Bilginin imhasına ilişkin bir tutanak hazırlanarak İngilizce çevirisi ile birlikte Kaynak Tarafın Güvenlik Makamına teslim edilecektir.

7. İşbu Anlaşma uyarınca oluşturulan ya da transfer edilen Gizlilik Dereceli Bilgini korunmasını ve iadesini imkânsız kılan bir durumda, Gizlilik Dereceli Bilgi derhal imha edilecektir. Alan Taraf, Kaynak Tarafın Yetkili Güvenlik Makamını mümkün olan en kısa zamanda imha hakkında bilgilendirecektir.

MADDE 8
GİZLİLİK DERECELİ SÖZLEŞMELER

1. İhale Makamı, Gizlilik Dereceli Sözleşme akdedilmeden önce kendi Yetkili Güvenlik Makamından, Yüklenicinin erişmesi gereken Gizlilik Dereceli Bilginin güvenlik tasnif derecesine uygun geçerli bir Tesis Güvenlik Belgesine sahip olduğunun diğer Tarafın Yetkili Güvenlik Makamınca doğrulanmasını talep etmesini isteyecektir.

2. HİZMETE ÖZEL / RISERVATO / RESTRICTED Gizlilik Derecesini haiz bir sözleşmenin akdinden önce Tarafların Yetkili Güvenlik Makamları, Yüklenicinin kendi ulusal mevzuatında belirtilen güvenlik koşullarına uygunluğunu onaylayacaktır.

3. 1. ve 2. Fıkralarda bahsi geçen onaylar; Yüklenicinin, topraklarında bulunduğu Tarafın ulusal mevzuatında tanımlanan Gizlilik Dereceli Bilginin korunmasına yönelik koşulları haiz olduğunu belgelendirmek üzere gerekli tedbirlerin eşit seviyede alındığını taahhüt edecektir.

4. Gizlilik Dereceli Bilgi, 1. ve 2. Fıkralarda bahsi geçen onay alınıncaya kadar Yükleniciye verilmeyecektir.

5. İhale Makamı; Yüklenicinin, Gizlilik Dereceli bir Sözleşmenin uygulanma safhasında talep edilecek ve Gizlilik Dereceli sözleşmelerin ayrılmaz bir parçası olmak üzere, ÖZEL / RISERVATISSMO / CONFIDENTIAL ya da daha üstü, gizlilik derecesini haiz bilgiye erişimine yönelik Proje Güvenlik Talimatı yayımlayacaktır. Proje Güvenlik Talimatı başlıca şu güvenlik şartlarını ihtiva eder:

a) Güvenlik tasnif seviyeleri de dâhil olmak üzere, Gizlilik Dereceli Sözleşmeye ilişkin Gizlilik Dereceli Bilgi türlerinin listesi,
b) Gizlilik Dereceli Sözleşmenin uygulanma safhasında ortaya çıkan bilginin güvenlik tasnif seviyelerinin verilebilmesi için gerek duyulan kurallar.

6. İhale Makamı, Proje Güvenlik Talimatının bir kopyasını, kendi Yetkili Güvenlik Makamına, Yüklenicinin Tarafının Yetkili Güvenlik Makamları tarafından onaylanması maksadıyla iletmek üzere teslim edecektir.

7. Gizlilik Dereceli Bilgiye erişimin söz konusu olduğu Gizlilik Dereceli bir Sözleşme, ancak ve ancak Yüklenicinin Proje Güvenlik Talimatında belirtilen Gizlilik Dereceli Bilgiyi korumak için gerekli koşulları haiz olması durumunda yürütülebilecektir.

8. Alt yükleniciler, Yüklenici için belirlenen Gizlilik Dereceli Bilginin Korunmasına yönelik koşullara tam olarak uymakla yükümlüdür.

9. Taraflar, Gizlilik Dereceli Sözleşmenin içeriğindeki Gizlilik Dereceli Bilgiye ilişkin fikri mülkiyet haklarına, ulusal mevzuatları çerçevesinde, karşılıklı olarak saygı göstereceklerdir. Ayrıntı ve istisnalar Gizlilik Dereceli Sözleşmelerde belirtilebilecektir.

MADDE 9
GÜVENLİK İHLÂLİ

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

2. Taraflardan birinin Kaynak Taraf olduğu ya da Taraflar arasındaki işbirliği ile ortaya çıkan Gizlilik Dereceli Bilginin güvenliğinin ihlal edilmesi veya ihlalinden şüphe edildiği durumlarda ihlalin gerçekleştiği ya da şüphenin oluştuğu Tarafın Yetkili Güvenlik Makamları derhal bilgilendirilecektir.

3. Güvenlik ihlali şüphesinin oluşması ya da gerçekleşmesi durumunda, soruşturma ortaya çıktığı Taraf ülkenin ulusal düzenlemelerine uygun olarak tahkik edilecektir.

4. Güvenlik ihlali olması durumunda, ihlalin gerçekleştiği Tarafın Yetkili Güvenlik Makamı karşı Tarafın Yetkili Güvenlik Makamını ihlal hakkındaki gerçekleri, ihlalin gerçekleştiği koşulları ve 9. Maddenin 3. Fıkrasında belirtilen faaliyetlerin sonuçlarını yazılı olarak bilgilendirmekle yükümlüdür.

5. Tarafların Yetkili Güvenlik Makamları, taraflardan birinin talep etmesi halinde 9. Maddenin 3. Fıkrasında belirtilen hususların icrasında işbirliği yapacaklardır.

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 gerçekleştirilebilecektir.

2. Ziyaret talepleri, ön görülen ziyaret tarihinin 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 talepler aşağıdaki bilgileri içerecek şekilde her bir ziyaret için ayrı ayrı hazırlanacaktır.
   a. Konuk personelin adı ve soyadı, doğum yeri ve tarihi, uyruğu, pasaport numarası ve görevi,
   b. Öngörülen ziyaret tarihi, program ve tahmini ziyaret süresi,
   c. Kişi Güvenlik Belgesi erişilmek istenen Gizlilik Dereceli Bilginin türü ve Gizlilik Derecesi.
   d. Ziyaret edilecek yerlerin, binaların 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 mührü, imzası ve istek tarihi.

4. Ziyaret izni yalnızca belirli bir tarih veya süre için geçerli olmalıdır. Ancak, işbirliğinde kolaylık sağlamak maksadıyla, 12 (oniki) ayı geçmeyen zaman dilimini kapsayan bir ziyaret programı oluşturulabilir. Bu durumda, planlanan ziyaretin müsaade edilen süre zarfında sonlandırılmayacağı öngörülürse ve bu tür ziyaretlerin sürelerinin uzatılması gerekliliği doğarsa ziyaret talebi, misafir personeli gönderen ülkenin Yetkili Güvenlik Kuruluşu tarafından, süregelen ziyaret izninin bitiş süresinden en az 21 (yirmibir) gün önce yenilenmelidir.

5. 3. Fıkrada bahsi geçen kişisel verileri korumak amacıyla, tarafların ulusal mevzuatlarına uygun olarak, aşağıda yer alan hükümler uygulanacaktır:

a. Ev Sahibince alınan kişisel veri yalnızca bu verileri aktaran Tarafça tanımlanan amaç ve koşullar çerçevesinde kullanılabilecektir.
b. Kişisel veriler, sadece amacı doğrultusunda ve istenilen amaca ulaşabilmek maksadıyla yapılacak gerekli işlemler süresince Ev Sahibi tarafından saklanacaktır. Kişisel veriler, ev sahibi tarafça sadece işleme konma amacının gerçekleştirilmesi için ve gerekli olduğu sürece saklanacaktır.
c. Kişisel verilerin ulusal mevzuatına aykırı olarak aktarılması durumunda, veriyi aktaran taraf, söz konusu verinin kısmi ya da tamamen yeniden yapılandırmasını engelleyecek şekilde imha edilmesi hususunda Ev Sahibi ülkeye bildirimde bulunacaktır.
d. Kişisel verileri gönderen taraf, verilerin doğruluğundan sorumludur. Verilerin yanlış veya eksik olduğunun anlaşılması halinde, bu verilerin düzeltilmesi veya ortadan kaldırılması amacıyla karşı tarafı uyaracaktır.
e. Taraflar, bu verilerin aktarılması, alınması ve imha edilmesini kayıt altına alacaktır.

MADDE 11
DİLLER

1. İşbu Anlaşmada belirtilen koşulların icrası kapsamında, Taraflar İngilizce ya da kendi resmi dillerini kullanacaklardır. Tarafların kendi dillerini kullanmaları durumunda ise diğer tarafın resmi dili ya da İngilizce çevirisi eklenecektir.

2. Oluşabilecek ihtilaflarda İngilizce metin esas alınacaktır.

MADDE 12
MALİ KONULAR

1. İşbu Anlaşmanın uygulanmasında, ilke olarak, hiçbir maliyet söz konusu değildir.

2. 1. Fıkrası ihlal edilmemek üzere, Taraflar işbu Anlaşmanın uygulanması sürecinde doğacak masrafları kendileri karşılayacaktır.

MADDE 13
İSTİŞARE VE TADİL

1. Taraflardan biri diğer Tarafa diplomatik kanallardan yazılı bildirim göndererek işbu Anlaşma üzerinde müzakere talep edebilir ve/veya tadil önerebilir.
2. İşbu Anlaşma, müzakere temelinde Tarafların karşılıklı yazılı onayı ile tadil edilebilir. Söz konusu olan tadiller, Madde 17'de belirtilen yasal usuller çerçevesinde yürürlüğe girecektir.

3. Tarafların Yetkili Güvenlik Kuruluşları, işbu Anlaşmanın yürürlüğüne yönelik kendi yasal düzenlemelerinde Gizlilik Dereceli Bilgilerin Korunması kapsamında yapılacak olası değişiklikler hakkında birbirlerini haberdar edeceklerdir.

4. İşbu Anlaşmanın amacı olan etkin işbirliğinin sağlanabilmesi ve Taraflarının ulusal mevzuatlarınca verilen yetki kapsamında Yetkili Güvenlik Makamları, gerekli hallerde, usul ve uygulamaya yönelik teknik düzenlemeleri yazılı mutabakat ile akdedebilir.

MADDE 14
UYUŞMAZLIKLARIN ÇÖZÜMÜ

1. İşbu Anlaşmanın uygulanmasına yönelik herhangi bir uyuşmazlık Tarafların Yetkili Güvenlik Kuruluşları arasında yürütülecek olan doğrudan müzakerelerle çözüme kavuşturulacaktır. Uyuşmazlıklar çözüm amacıyla herhangi bir ulusal, uluslararası mahkemeye veya Üçüncü Tarafa intikal ettirilmeyecektir.

2. Uyuşmazlığın 1. Fıkrada belirtildiği şekilde çözümlenememesi halinde, bu tür uyuşmazlıklar diplomatik kanallarla çözümlenecektir. Yazılı bildirim alındığı tarihten sonra 45 (kırkbeş) gün içinde çözüme ulaşılamaması halinde, her iki Taraf da bu Anlaşmayı fesih edebilir.

3. Taraflar, doğrudan ya da diplomatik kanallarla yürütülmekte olan görüşmeler süresince işbu Anlaşmanın koşullarını uygulamaya devam edeceklerdir.

MADDE 15
HUKUKSAL UYGUNLUK

Bu Anlaşma, her iki tarafın ulusal mevzuatlarına, taraf oldukları uluslararası anlaşmalara ve tarafların uluslararası kuruluşlara, bölgesel veya alt bölgesel birlik ve kuruluşlara katılımlarından doğan yükümlülüklerine uygun olarak uygulanacaktır.

MADDE 16
YÜRÜRLÜK SÜRESİ VE SONA ERDİRME

1. İşbu Anlaşmanın yürürlük süresi 5 (beş) yıl olarak akdedilmiş olup taraflar fesih taleplerini yürürlük süresinin sona ermesinden en geç 30 (otuz) gün öncesine kadar diplomatik kanalları aracılığı ile iletmedikleri takdirde işbu Anlaşma beş yıllık sürelerle otomatik olarak yenilenecektir.

2. Taraflardan biri diğer Tarafa konu ile ilgili yazılı bir bildirimi diplomatik kanallarla göndermek suretiyle işbu Anlaşmayı dilediği zaman feshedebilir. Böyle bir durumda, işbu Anlaşma fesih bildiriminin alımını takip eden 3 (üç) ay sonunda sona erecektir. İşbu Anlaşmanın sona ermesi durumunda, işbu Anlaşma kapsamında mübadele edilen ya da oluşturulan Gizlilik Dereceli Bilgiler burada geçen hükümler uyarınca daimi olarak korunacaktır.

3. Uyuşmazlıklar konusunda çözüme ulaşılamaması durumunda, taraflar kendi istekleri doğrultusunda işbu Anlaşmayı feshedebilirler.

MADDE 17
YÜRÜRLÜĞE GİRİŞ

İşbu Anlaşma, Tarafların Anlaşmanın yürürlüğe girmesi için gerekli ulusal yasal düzenlemelerin tamamlandığını birbirlerine karşılıklı diplomatik yollarla bildirdikleri son yazılı bildirimin alındığı tarih itibariyle yürürlüğe girer.

MADDE 18
METİN VE İMZA

1. 5 Temmuz tarihinde Ankara'da her biri eşit derecede geçerli olmak üzere İtalyanca, Türkçe ve İngilizce dillerinde ikişer asıl nüsha olarak imzalanmıştır. İşbu Anlaşma hükümlerinin yorumlanması ile ilgili uyuşmazlıklarda İngilizce metin esas alınacaktır.

2. İşbu Anlaşma aşağıda imzası bulunan yetkilendirilmiş temsilciler tarafından imzalanmıştır.

İTALYAN CUMHURİYETİ HÜKÜMETİ ADINA

İMZA:

İSİM:

UNVAN:

TÜRKİYE CUMHURİYETİ HÜKÜMETİ ADINA

İMZA:

İSİM:

UNVAN:

AGREEMENT

BETWEEN

THE GOVERNMENT OF THE ITALIAN REPUBLIC

AND

THE GOVERNMENT OF THE REPUBLIC OF TÜRKİYE

ON MUTUAL PROTECTION OF CLASSIFIED INFORMATION

IN DEFENCE INDUSTRY

INTRODUCTION

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

Taking into consideration the articles of the "Memorandum of Understanding Regarding Cooperation in the Defence Material Sector" signed on 15th June 1988,

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 and mutual protection of Classified Information related to 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 exchange and/or joint production,

Subject to the national laws of the Parties,

Confirming that this Agreement shall not affect the rights and 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, originated and exchanged by the Parties, Competent Security Authorities, Authorized Entities, contractors and sub-contractors, in accordance with their respective national legislations.

ARTICLE 2
DEFINITIONS

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

1. Classified Information-any information related to defence industry, regardless of its form or nature, which requires protection against unauthorized access or manipulation and to which a security classification level has been assigned, in accordance to the national legislation of the Parties and this Agreement.

2. Competent Security Authority- the National Security Authority, competent for or duly authorised to deal with defence industry matters and responsible for implementation of this Agreement in accordance to the national legislation of the Parties, as specified in Article III of this Agreement.

3. Classified Contract- means an agreement between two or more contractors or sub-contractors, which includes or involves access to or creation of Classified Information; related to the defence industry.

4. Contractor- a natural person, a legal entity which under the law of one of the Parties, has legal capacity to perform Classified Contracts in accordance with the provisions of this Agreement.

5. Contracting Authority- means a legal entity or other form of organization under the law of one of the Parties,that has legal capacity to form Classified Contracts to Contractors or Sub-contractors in accordance with the provisions of this Agreement.

6. Facility Security Clearance- a document issued in accordance with the national legislation of a Party by the Competent Security Authority or other authorized entity and attesting that a Contractor has the physical and organizational capability to handle, store and protect Classified Information.

7. Principle of Need-to-Know- means the necessity to have access to Classified Information, Documents and Material in connection with Official Duty and/or for the performance of a concrete task.

8. Authorized Entities- The government agencies, legal entities, as well as natural persons, competent to handle Classified Information in accordance with their respective national legislations.

9. Originating Party- The Party, including natural or legal persons under its jurisdictions, which originates or transmits Classified Information to the Receiving Party.

10. Recipient Party- The Party, including natural or legal persons under its jurisdictions which receives Classified Information from the Originating Party.

11. Personnel Security Clearance- A document issued in accordance with the national legislation of a Party by the Competent Security Authority or other Designated Security Authority 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 Italian Republic: National Security Authority, Department of Security and Information - Central Secrecy Office.
   2) for the Republic of Türkiye: Ministry of National Defence of the Republic of Türkiye, Directorate General for Technical Services;

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

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 under the jurisdictions of the Parties commit to duly ensure the protection of the Classified Information exchanged between each other or generated by mutual cooperation, using equivalence of levels of classification as shown in the table below in Italian, Turkish and English:

in Italian	in Turkish	in English
"SEGRETISSIMO"	"ÇOK GİZLİ"	"TOP SECRET"
"SEGRETO"	"GİZLİ"	"SECRET"
"RISERVATISSMO"	"ÖZEL"	"CONFIDENTIAL"
"RISERVATO"	"HİZMETE ÖZEL"	"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 equivalent level of national security classification in English and in its own language in accordance with the table above.

3. The relevant Competent Security Authorities shall inform each other of respective national legislation on Classified Information and any significant amendments thereto, and shall exchange information about the security standards, procedures and practices for the protection of Classified Information.

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/exchanged or originated as a result of cooperation between the Parties, including this document originated in connection with the implementation 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 accessed and handled only by persons who have a need-to-know on the basis of their duties 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 mutually recognize Personnel Security Clearances (PSCs) and Facility Security Clearances(FSCs) issued in accordance with the national legislation of the other Party. The Parties should also cooperate and ensure mutual support in carrying out vetting procedures and exchanging of information needed to release PSCs and FSCs.

ARTICLE 6
TRANSFER OF THE CLASSIFIED INFORMATION

1. Classified Information marked as ÇOK GİZLİ / SEGRETISSIMO / TOP SECRET level shall be exchanged via diplomatic channels in accordance to the national legislation of the Parties. As a minimum level such Classified Information shall be carried by, and under the sole control of a Government courier holding a Personal Security Clearance at ÇOK GİZLİ / SEGRETISSIMO / TOP SECRET level. The Receiving Party shall confirm the receipt of as ÇOK GİZLİ / SEGRETISSIMO / TOP SECRET Classified Information in writing.

2. Classified Information up to GİZLİ / SEGRETO / SECRET shall be transmitted via diplomatic channels or military attaché.

3. Information classified as HİZMETE ÖZEL / RISERVATO / RESTRICTED may be transmitted also through authorized carriers in accordance with the national legislation of the Originating Party.

4. 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 / RISERVATO / RESTRICTED by authorized individuals is admissible.

5. 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. 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 at ÇOK GİZLİ / SEGRETISSIMO / TOPSECRET level, both in original form and translation, shall be translated or reproduced only upon prior written consent of the Competent Security Authority of the country of the Originating Party.

2. All translations shall bear 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. Classified Information shall be destroyed in a way that prevents its partial or total reconstruction.

4. Classified Information marked up to GİZLİ / SEGRETO / SECRET shall be destroyed in accordance to the national legislation of the Parties.

5. Classified Information marked as ÇOK GİZLİ / SEGRETISSIMO / TOP SECRET shall not be destroyed. It shall be returned to Security Authority of the Originating Party.

6. Along with its translation in English, a report on destruction of Classified Information shall be made and delivered to the Security Authority of the Originating Party.

7. In case of a crisis situation in which it is impossible to protect or return Classified Information it shall be destroyed immediately. The Receiving Party shall inform the Security Authority of the Originating Party about this destruction as soon as possible.

ARTICLE 8
CLASSIFIED CONTRACTS

1. Before concluding a Classified Contract, the Contracting Authority shall demand to its Competent Security Authority to request the Competent Security Authority of the other Party to confirm that the Contractor holds a valid Facility Security Clearance corresponding to the security classification level of the Classified Information to which the Contractor is to have access.

2. Before concluding a Classified Contract involving information classified as HİZMETE ÖZEL / RISERVATO / 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 Contracting Authority shall publish a project security instruction(PSI) necessary to perform a Classified Contract connected with access to information classified as ÖZEL / RISERVATISSMO / CONFIDENTIAL or above, which is an integral part of such Classified Contract. The project security instruction contains provisions on the security requirements, in particular:

a) the list of types of Classified Information related to a given Classified Contract, including their security classification levels;
b) the criteria based on which classification levels are attributed to information originated during the performance of a given Classified Contract.

6. The Contracting Authority shall submit 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 for approval.

7. The performance of a Classified Contract with regard to 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 foreseen 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.

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 any suspected or actual breach of security concerning Classified Information originated by one of the Parties 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. Any suspected or actual 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 of Article 9.

5. The Competent Security Authorities of the Parties shall cooperate in the actions referred to in Paragraph 3 of Article 9, 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 set 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 only in order to and as long as it is necessary to achieve the purpose of its processing;
c. in case of personal data transmitted against the national law 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. In case a data appears to be untrue or incomplete, the other party shall be notified in order to correct or remove the data;
e. Parties shall register transmission, receipt and removal of the data.

ARTICLE 11
LANGUAGES

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

2. In case of conflicting interpretations, the interpretation of the English text shall prevail.

ARTICLE 12
FINANCIAL MATTERS

1. The implementation of this Agreement does not include, in principle, any cost.

2. Without prejudice to Paragraph 1, each Party shall bear its possible unexpected expenses related to the implementation 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 through diplomatic channels.

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 17.

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.

4. 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 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 dispute shall be settled via negotiations through diplomatic channels. If a solution is not reached within 45 (forty-five) days after the receipt of the written notification, each Party may terminate this Agreement.

3. Pending negotiations, either direct or via diplomatic channels, the Parties shall continue to apply the provisions of this Agreement.

ARTICLE 15
APPLICABLE LAW

This Agreement shall be implemented in accordance with the national legislations of both Parties, the international agreements to which they are parties and obligations of the Parties arising from their participation in international organisations, the regional or sub-regional union and entities.

ARTICLE 16
EFFECTIVENESS PERIOD AND TERMINATION

1. This Agreement is concluded for 5 (five) years and it shall be renewed automatically for successive periods of five years, unless one of the Parties notifies the other in writing through diplomatic channels of its intention to terminate the Agreement 30 (thirty) days prior to its expiration.

2. Each Party may terminate this Agreement at any time by giving the other Party a written notification to that effect through diplomatic channels. In this case, this Agreement shall be terminated 3 (three) months after the date of the receipt of the notification. 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.

3. In the case of dispute, if a solution is not reached, each Party may terminate this Agreement.

ARTICLE 17
ENTRY INTO FORCE

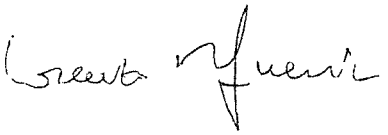
This Agreement shall enter into force on the date of receipt of the last written notification by which the Parties notify each other, through diplomatic channels, of the completion of their internal legal procedures required for the entry into force of the Agreement.

ARTICLE 18
TEXT AND SIGNATURE

1. Done at Ankara on the 5th of July 2022, in two originals in the Italian, Turkish and English languages, all texts being equally authentic. In case of any dispute regarding the interpretation of provisions of this Agreement, the text in English shall prevail.

2. In witness whereof, the undersigned, being duly authorized thereto, have signed this Agreement.

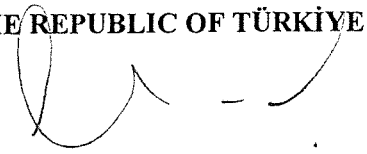
FOR THE GOVERNMENT OF THE ITALIAN REPUBLIC

SIGNATURE: 

NAME:

TITLE:

FOR THE GOVERNMENT OF THE REPUBLIC OF TÜRKİYE

SIGNATURE: 

NAME:

TITLE: