ACCORDO TRA IL GOVERNO DELLA REPUBBLICA ITALIANA E IL GOVERNO DELLA REPUBBLICA DI CIPRO SULLO SCAMBIO E LA RECIPROCA PROTEZIONE DELLE INFORMAZIONI CLASSIFICATE

Il Governo della Repubblica Italiana
e
il Governo della Repubblica di Cipro

(qui di seguito denominate "le Parti"),

Riconoscendo la necessità di stabilire regole sulla protezione delle Informazioni Classificate reciprocamente scambiate nell'interesse della sicurezza nazionale nell'ambito di cooperazione politica, militare, economica, giuridica, scientifica e tecnologica o ogni altro tipo di cooperazione, oltre alle Informazioni Classificate prodotte nel contesto di tali forme di cooperazione;

Intendendo assicurare la reciproca protezione di tutte le Informazioni Classificate che sono state classificate da una delle Parti e trasmesse all'altra Parte o congiuntamente prodotte nel corso della cooperazione tra le Parti;

Desiderando creare un serie di norme sulla reciproca protezione delle Informazioni Classificate scambiate tra le Parti;

Considerando gli interessi comuni alla protezione delle Informazioni Classificate, in conformità con la normativa delle Parti;

Hanno concordato quanto segue:

Articolo 1
Scopo

Lo scopo di questo Accordo è di assicurare la protezione delle Informazioni Classificate prodotte o reciprocamente scambiate tra le Parti o tra i contraenti o subcontraenti o tra ogni altra persona giuridica pubblica o privata autorizzata a trattare e custodire le Informazioni Classificate.

Articolo 2
Definizioni

Ai fini di questo Accordo:

"**Violazione di Sicurezza**" indica un atto o una omissione contraria a questo Accordo o alla legislazione nazionale delle Parti, il cui risultato può causare il disvelamento, la perdita, la distruzione, l'appropriazione indebita o ogni altro tipo di compromissione dell'Informazione Classificata.

"**Contratto Classificato**" indica un accordo tra due o più Contraenti o subcontraenti, che contiene Informazioni Classificate o ne implica l'accesso o la creazione.

"**Informazione Classificata**" indica ogni informazione a prescindere dalla sua forma o natura, che richiede la protezione dall'accesso o dalla manipolazione non autorizzata e alla quale è stato assegnato un livello di classifica di segretezza, in conformità con la legislazione nazionale delle Parti.

"**Autorità di Sicurezza Competente**" indica ogni autorità competente delle Parti, oltre alle Autorità Nazionali di Sicurezza, che in conformità con la propria legislazione nazionale, è responsabile dell'attuazione del presente Accordo.

"**Contraente**" indica una persona giuridica che ha capacità legale di concludere o eseguire dei contratti.

"**Abilitazione di Sicurezza Industriale**" indica la favorevole decisione adottata dall'Autorità di Sicurezza che attesta che la persona giuridica ha la capacità fisica e organizzativa di trattare e custodire le Informazioni Classificate in conformità con le legislazioni nazionali di entrambe le Parti.

"**Autorità Nazionale di Sicurezza**" indica l'autorità statale di ogni Parte che, in conformità con la propria legislazione nazionale è responsabile, in senso generale, dell'attuazione e della supervisione del presente Accordo; le rispettive autorità delle Parti sono menzionate nell'Articolo 4 paragrafo 1 del presente Accordo.

"**Necessità di conoscere**" indica il principio in base al quale l'accesso a specifiche Informazioni Classificate è accordato esclusivamente in relazione all'incarico ufficiale ricevuto e all'esecuzione di uno specifico compito.

"**Parte Fornitrice**" indica la Parte che fornisce l'Informazione Classificata alla Parte Ricevente.

"**Abilitazione di Sicurezza Personale**" indica la decisione favorevole adottata dall'Autorità di Sicurezza, che conferma, in conformità con la rispettiva legislazione nazionale delle Parti, che una persona è autorizzata ad avere accesso e trattare Informazioni Classificate fino ad uno specifico livello.

"**Parte Ricevente**" indica la Parte alla quale l'informazione classificata è trasmessa.

"**Parte Terza**" indica ogni Stato, organizzazione, persona fisica o giuridica che non è parte di questo Accordo

Articolo 3
Livelli di Classifica di Segretezza

Le Parti concordano che i seguenti livelli di classifica di segretezza e contrassegni sono equivalenti e corrispondono ai livelli di classifica di segretezza previsti nella loro legislazione nazionale:

SEGRETISSIMO	ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ	TOP SECRET
SEGRETO	ΑΠΟΡΡΗΤΟ	SECRET
RISERVATISSIMO	ΕΜΠΙΣΤΕΥΤΙΚΟ	CONFIDENTIAL
RISERVATO	ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ	RESTRICTED

Articolo 4
Autorità di Sicurezza

1. Le Autorità Nazionali di Sicurezza delle Parti sono:

   Per la Repubblica Italiana:
   Presidenza del Consiglio dei Ministri – Dipartimento delle Informazioni per la Sicurezza (DIS) – UCSe;

   Per la Repubblica di Cipro:
   Autorità Nazionale di Sicurezza
   Ministero della Difesa della Repubblica di Cipro.

2. Le Parti si informano reciprocamente attraverso canali diplomatici di ogni modifica concernente le Autorità Nazionali di Sicurezza.
3. Su richiesta, le Autorità Nazionali di Sicurezza si comunicano reciprocamente le altre Autorità di Sicurezza.
4. Le Autorità Nazionali di Sicurezza si informano reciprocamente in merito alle rispettive normative nazionali riguardanti le Informazioni Classificate e ad ogni significativa modifica delle stesse e si scambiano informazioni circa i criteri, le procedure e le prassi di sicurezza per la protezione delle informazioni classificate.

Articolo 5
Misure di Protezione e Accesso alle Informazioni Classificate

1. In conformità con le rispettive legislazioni nazionali, le Parti adottano tutte le misure necessarie per la protezione delle Informazioni Classificate generate o scambiate ai sensi del presente accordo. Le Parti assegnano, alle Informazioni Classificate create e/o fornite ai sensi del presente Accordo, lo stesso livello di protezione che assegnerebbero alle proprie Informazioni Classificate secondo i livelli di classifica di segretezza, così come definiti nell'Articolo 3.
2. La Parte fornitrice informa:
   a) la Parte ricevente di ogni condizione di rilascio o limitazione all'utilizzo delle Informazioni Classificate;
   b) la Parte Ricevente per iscritto di ogni cambiamento del livello di classifica di segretezza dell'Informazione Classificata trasmessa.
3. L'accesso alle Informazioni classificate a livello RISERVATISSIMO/ ΕΜΠΙΣΤΕΥΤΙΚΟ/CONFIDENTIAL e superiore è limitato alle persone fisiche e giuridiche in possesso di una abilitazione di sicurezza di livello adeguato rilasciata sulla base della Necessità di Conoscere in conformità con la legislazione nazionale delle Parti.
4. L'Abilitazione di Sicurezza Personale non è richiesta per l'accesso a informazioni Classificate contrassegnate RISERVATO/ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ/ RESTRICTED. Tale accesso è consentito alle sole persone fisiche che hanno la Necessità di Conoscere e sono state debitamente indottrinate sulle loro responsabilità ed obblighi di protezione di tali Informazioni Classificate.
5. Nell'ambito dello scopo del presente Accordo, ogni Parte riconosce le Abilitazioni di Sicurezza Personali e la Abilitazioni di Sicurezza Industriali rilasciate dall'altra Parte in conformità con la legislazione nazionale. Le abilitazioni di Sicurezza devono essere equivalenti ai livelli previsti dall'articolo 3.

6. Le Autorità Nazionali per la Sicurezza si assistono reciprocamente, previa richiesta ed in conformità con le normative nazionali, nell'esecuzione delle indagini di sicurezza necessarie per l'applicazione del presente Accordo.
7. Nell'ambito dello scopo del presente Accordo, le Autorità di Sicurezza delle Parti si informano reciprocamente e con tempestività di ogni modifica delle Abilitazioni di Sicurezza Personali ed Industriali, in particolare nei casi di revoca o abbassamento del livello delle stesse.
8. La Parte Ricevente deve:
   a) rilasciare le Informazioni Classificate a Parti Terze solo previo consenso scritto della Parte Fornitrice;
   b) contrassegnare l'Informazione Classificata ricevuta in conformità con quanto previsto dall'articolo 3;
   c) utilizzare l'Informazione Classificata solo per gli scopi per cui la stessa è stata fornita.

Articolo 6
Trasmissione di informazioni classificate

1. Le Informazioni Classificate a livello SEGRETISSIMO / ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ / TOP SECRET sono trasmesse attraverso canali governativi in conformità con le legislazioni nazionali delle Parti. Quale livello minimo di sicurezza, tali Informazioni Classificate sono trasportate da un corriere Governativo in possesso di Abilitazione di Sicurezza Personale a livello SEGRETISSIMO/ ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ/ TOP SECRET e sottoposte al solo controllo di quest'ultimo. La Parte Ricevente conferma per iscritto la ricezione delle Informazioni Classificate SEGRETISSIMO / ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ / TOP SECRET.
2. Le Informazioni Classificate a livello SEGRETO /ΑΠΟΡΡΗΤΟ / SECRET o RISERVATISSIMO / ΕΜΠΙΣΤΕΥΤΙΚΟ / CONFIDENTIAL sono trasmesse attraverso canali governativi in conformità con la normativa nazionale delle Parti ovvero attraverso altri canali protetti, reciprocamente approvati dalle Autorità di Sicurezza di entrambe le Parti. La Parte Ricevente conferma per iscritto la ricezione delle Informazioni Classificate a livello SEGRETO /ΑΠΟΡΡΗΤΟ / SECRET e / RISERVATISSIMO / ΕΜΠΙΣΤΕΥΤΙΚΟ / CONFIDENTIAL.
3. Le Informazioni Classificate a livello RISERVATO / ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ / RESTRICTED sono trasmesse attraverso canali protetti in conformità con la normativa nazionale delle Parti.
4. In caso di spedizioni di grandi dimensioni contenenti Informazioni Classificate, le procedure di trasporto sono concordate e valutate, caso per caso, dalle Autorità Nazionali per la Sicurezza di entrambe le Parti.
5. Le Informazioni Classificate a livello SEGRETO / ΑΠΟΡΡΗΤΟ /SECRET, RISERVATISSIMO / ΕΜΠΙΣΤΕΥΤΙΚΟ CONFIDENTIAL e RISERVATO/ ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ/ /RESTRICTED trasmesse in forma elettronica tra le Parti, non devono essere inviate sotto forma di testo in chiaro. La trasmissione elettronica di questi specifici livelli di Classifica di Segretezza è effettuata mediante mezzi crittografici certificati, reciprocamente approvati dalle Autorità Nazionali per la Sicurezza.
6. I punti di ingresso e di uscita principali per lo scambio di Informazioni Classificate ai sensi del presente accordo sono:

   Per la Repubblica Italiana:

a) quelli previsti dalla normativa nazionale;

b) l'Autorità Nazionale per la Sicurezza si impegna a fornire al Ministero degli Affari Esteri della Repubblica di Cipro un elenco aggiornato dei punti di sicurezza di ingresso e di uscita delle Informazioni Classificate dei soggetti considerati "pubblici" ai sensi della normativa italiana.

Per la Repubblica di Cipro:
Il Central TOP SECRET Registry presso il Ministero degli Affari Esteri.

Articolo 7
Riproduzione e Traduzione di Informazioni Classificate

1. Le traduzioni e le riproduzioni di Informazioni Classificate sono effettuate in conformità con la normativa nazionale della Parte Ricevente e secondo le seguenti procedure:
   a) le traduzioni e le riproduzioni sono contrassegnate e protette come le Informazioni Classificate originali;
   b) le traduzioni e il numero delle copie sono limitate a quelle strettamente necessarie ai fini ufficiali;
   c) le traduzioni recano un'appropriata annotazione nella lingua della traduzione, indicante che essa contiene Informazioni Classificate ricevute dalla Parte Fornitrice.
2. Le Informazioni Classificate a livello SEGRETO / ΑΠΟΡΡΗΤΟ / SECRET o superiore sono tradotte o riprodotte solo previa autorizzazione scritta della Parte Fornitrice.

Articolo 8
Distruzione delle Informazioni Classificate

1. Le Informazioni Classificate vengono distrutte in modo da impedirne la ricostruzione parziale o totale.
2. Le Informazioni Classificate fino al livello SEGRETO / ΑΠΟΡΡΗΤΟ / SECRET sono distrutte in conformità alla normativa nazionale delle Parti.
3. Le Informazioni Classificate a livello SEGRETISSIMO / ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ / TOP SECRET non vengono distrutte. Esse sono restituite all'Autorità di Sicurezza della Parte Fornitrice.
4. Una relazione sulla distruzione delle Informazioni Classificate è redatta e la relativa traduzione in inglese è inviata all'Autorità di Sicurezza della Parte Fornitrice.
5. In caso di situazioni di crisi in cui è impossibile proteggere o restituire le Informazioni Classificate, esse devono essere distrutte immediatamente. La Parte Ricevente informa appena possibile l'Autorità di Sicurezza della Parte Fornitrice circa l'avvenuta distruzione.

Articolo 9
Contratti Classificati

1. L'Autorità Nazionale per la Sicurezza di una Parte garantisce preventivamente e per iscritto all'Autorità Nazionale per la Sicurezza dell'altra Parte che un contraente o un subcontraente, che intenda stipulare un Contratto Classificato a livello RISERVATISSIMO / ΕΜΠΙΣΤΕΥΤΙΚΟ / CONFIDENTIAL e SEGRETO/ ΑΠΟΡΡΗΤΟ / SECRET con l'altra Parte, detiene o è in procinto di ottenere un'Abilitazione di Sicurezza Industriale del livello di classifica di segretezza adeguato.
2. Ogni Contratto Classificato ai sensi del presente Accordo comprende:

a) l'impegno a rispettare le disposizioni del presente Accordo;

b) l'impegno del Contraente o del subcontraente a garantire che i loro locali possiedano le condizioni necessarie per la trattazione e la custodia di Informazioni Classificate di un determinato livello di classifica segretezza;

c) l'impegno del Contraente o del subcontraente a garantire che le persone che svolgono funzioni che richiedono l'accesso a Informazioni Classificate siano debitamente autorizzate, in conformità con la loro normativa nazionale, all'accesso alle Informazioni Classificate del livello di classifica equivalente ed abbiano ricevuto una regolare istruzione di sicurezza;

d) la lista delle Informazioni Classificate e l'elenco delle aree in cui le Informazioni Classificate possono essere conservate trattate e custodite;

e) l'impegno a comunicare qualsiasi modifica del livello di classifica di segretezza delle Informazioni Classificate;

f) la procedura per la trasmissione delle Informazioni Classificate;

g) l'impegno del Contraente o del subcontraente a notificare alla propria Autorità Nazionale per la sicurezza ogni violazione della sicurezza, sia essa reale o sospetta;

h) l'impegno del Contraente o del subcontraente a fornire una copia del Contratto Classificato alle Autorità Nazionali per la Sicurezza di entrambe le Parti.

3. Per i Contratti classificati che implicano l'accesso ad Informazioni Classificate di livello di non superiore a RISERVATO / ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ /RESTRICTED non è richiesta alcuna Abilitazione di Sicurezza Industriale e/o Abilitazione di Sicurezza Personale. Tali Contratti Classificati contengono un'appropriata clausola sui requisiti di sicurezza che definisce le condizioni minime di sicurezza che il Contraente deve applicare per le Informazioni Classificate generate e/o fornite in ragione del Contratto. La clausola di sicurezza deve includere una disposizione relativa alla nomina, da parte del Contraente, di una persona che abbia la responsabilità generale della protezione delle Informazioni Classificate a livello / RISERVATO / ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ /RESTRICTED. Solo se richiesta, una copia della disposizione sui requisiti di sicurezza è fornita all'Autorità Nazionale per la Sicurezza.

4. Ai soli fini della sicurezza industriale, ai sensi della normativa italiana, i punti di ingresso e di uscita delle Informazioni Classificate, a norma dell'articolo 6, paragrafo 6, del presente Accordo, sono gli organi di sicurezza dei Contraenti o dei subcontraenti muniti di Abilitazione di Sicurezza Industriale.

Articolo 10
Visite Classificate

1. Le visite ufficiali governative che comportano l'accesso ad Informazioni Classificate a livello SEGRETISSIMO / ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ / TOP SECRET, /SEGRETO / ΑΠΟΡΡΗΤΟ / SECRET e RISERVATISSIMO /ΕΜΠΙΣΤΕΥΤΙΚΟ /CONFIDENTIAL devono essere effettuate previa presentazione di un'Abilitazione di Sicurezza Personale.

2. Ai fini del presente Accordo, tutte le altre tipologie di visite, non disciplinate dal paragrafo 1, che prevedono l'accesso a Informazioni Classificate a livello RISERVATISSIMO / ΕΜΠΙΣΤΕΥΤΙΚΟ / CONFIDENTIAL e SEGRETO/ ΑΠΟΡΡΗΤΟ / SECRET sono soggette ad una preventiva autorizzazione scritta rilasciata dall'Autorità Nazionale per la Sicurezza della Parte ospitante.

3. L'Autorità Nazionale per la Sicurezza della Parte ospitante deve ricevere una richiesta di visita con almeno 20 (venti) giorni di anticipo.
4. Nei casi urgenti, la richiesta di visita può essere trasmessa in tempi più brevi.
5. La richiesta di visita deve riportare:
   a) il nome e cognome, il luogo e data di nascita, la cittadinanza, il numero di passaporto o di documento di identità del visitatore;
   b) il nome della persona giuridica rappresentata dal visitatore ed l'incarico del visitatore nell'ambito di detta persona giuridica;
   c) il nome, l'indirizzo ed il punto di contatto della persona giuridica e della struttura da visitare;
   d) la conferma dell'Abilitazione di Sicurezza Personale del visitatore, della sua validità e del relativo livello;
   e) l'oggetto e lo scopo della visita e l'indicazione del più alto livello di classifica di segretezza delle Informazioni Classificate interessate;
   f) la data e la durata prevista della visita richiesta. In caso di visite ricorrenti, è indicato il periodo totale coperto dalle visite;
   g) la data, la firma ed il timbro del competente organo di sicurezza.
6. Una volta autorizzata la visita l'Autorità Nazionale per la Sicurezza della Parte ospitante fornisce una copia della richiesta di visita al funzionario alla sicurezza della persona giuridica da visitare.
7. La validità dell'autorizzazione della visita non può essere superiore ad un anno.
8. Le Autorità Nazionali per la Sicurezza delle Parti possono predisporre elenchi di persone autorizzate ad effettuare visite ricorrenti. Tali elenchi sono validi per un periodo iniziale di dodici mesi. I dettagli delle rispettive visite sono organizzati direttamente con i competenti punti di contatto all'interno del soggetto giuridico da visitare, secondo i termini e le condizioni concordati.

Articolo 11
Violazioni della Sicurezza

1. In caso di Violazioni della Sicurezza l'Autorità Nazionale per la Sicurezza della Parte Ricevente informa quanto prima l'Autorità Nazionale per la Sicurezza della Parte Fornitrice e avvia la prevista indagine.
2. Qualora si verifichi una Violazione della Sicurezza in un paese terzo, l'Autorità Nazionale per la Sicurezza della Parte che ha ceduto l'informazione al paese terzo adotta tutte le misure necessarie per assicurare l'avvio delle azioni di cui al paragrafo 1.
3. La Parte Fornitrice, su richiesta, collabora all'inchiesta di cui al paragrafo 1.
4. La Parte Fornitrice è informata dei risultati dell'inchiesta e riceve la relazione finale sulle cause e sull'entità del danno.

Articolo 12
Spese

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

2. Fatta salva la disposizione del paragrafo 1, ciascuna Parte sostiene le eventuali spese impreviste originate nel corso dell'attuazione e della verifica del presente accordo.

Articolo 13
Risoluzione delle Controversie

Ogni controversia relativa all'interpretazione o all'applicazione del presente Accordo è risolta mediante negoziati tra le Parti.

Articolo 14
Disposizioni Finali

1. Il presente Accordo è valido per un periodo di tempo indeterminato ed entra in vigore il primo giorno del secondo mese successivo alla data di ricevimento dell'ultima notifica scritta, mediante la quale le Parti hanno notificato reciprocamente, tramite canali diplomatici, che gli adempimenti giuridici nazionali necessari per la sua entrata in vigore sono stati completati.
2. Il presente Accordo può essere modificato in qualsiasi momento sulla base del reciproco consenso scritto delle Parti. Le modifiche entrano in vigore conformemente a quanto disposto dal paragrafo 1.
3. Ciascuna parte può, in qualsiasi momento, denunciare il presente accordo mediante notifica scritta all'altra parte attraverso canali diplomatici. In questo caso, detta denuncia avrà effetto sei mesi dopo la data di ricevimento della relativa notifica.
4. In caso di denuncia del presente Accordo, le Parti assicurano che tutte le Informazioni Classificate continuano ad essere protette fino a quando la Parte Fornitrice non esonera la Parte Ricevente da tale obbligo.

Fatto a Nicosia..... il 31...luglio...2017..... in due esemplari originali, ciascuno in lingua italiana, greca e inglese, essendo tutti i testi ugualmente autentici. In caso di divergenze interpretative, prevale il testo in lingua inglese.

Per il Governo della Repubblica Italiana	**Per il Governo della Repubblica di Cipro**

ΣΥΜΦΩΝΙΑ

ΜΕΤΑΞΥ ΤΗΣ ΚΥΒΕΡΝΗΣΗΣ ΤΗΣ ΙΤΑΛΙΚΗΣ ΔΗΜΟΚΡΑΤΙΑΣ ΚΑΙ ΤΗΣ ΚΥΒΕΡΝΗΣΗΣ ΤΗΣ ΚΥΠΡΙΑΚΗΣ ΔΗΜΟΚΡΑΤΙΑΣ ΓΙΑ ΤΗΝ ΑΝΤΑΛΛΑΓΗ ΚΑΙ ΑΜΟΙΒΑΙΑ ΠΡΟΣΤΑΣΙΑ ΔΙΑΒΑΘΜΙΣΜΕΝΩΝ ΠΛΗΡΟΦΟΡΙΩΝ

Η Κυβέρνηση της Ιταλικής Δημοκρατίας
και
η Κυβέρνηση της Κυπριακής Δημοκρατίας

(εφεξής καλούμενες τα «Μέρη»),

Αναγνωρίζοντας την ανάγκη για τον καθορισμό κανόνων σχετικά με την προστασία Διαβαθμισμένων Πληροφοριών τις οποίες ανταλλάσσουν προς το συμφέρον της εθνικής ασφαλείας, στα πλαίσια πολιτικής, στρατιωτικής, οικονομικής, νομικής, επιστημονικής και τεχνολογικής ή άλλης συνεργασίας, καθώς και Διαβαθμισμένων Πληροφοριών που προκύπτουν από την εν λόγω συνεργασία;

Σκοπεύοντας να διασφαλίσουν την αμοιβαία προστασία όλων των Διαβαθμισμένων Πληροφοριών οι οποίες διαβαθμίστηκαν στο ένα Μέρος και διαβιβάστηκαν στο άλλο Μέρος ή που παράγονται από κοινού στα πλαίσια συνεργασίας μεταξύ των Μερών;

Επιθυμώντας να θεσπίσουν κανόνες για την αμοιβαία προστασία των Διαβαθμισμένων Πληροφοριών τις οποίες ανταλλάσσουν τα Μέρη μεταξύ τους;

Λαμβάνοντας υπόψη το αμοιβαίο συμφέρον της προστασίας των Διαβαθμισμένων Πληροφοριών, σύμφωνα με τη νομοθεσία των Μερών;

Συμφώνησαν τα ακόλουθα:

Άρθρο 1
Σκοπός

Σκοπός της παρούσας Συμφωνίας είναι η διασφάλιση της αμοιβαίας προστασίας Διαβαθμισμένων Πληροφοριών τις οποίες παράγουν από κοινού ή ανταλλάσσουν μεταξύ τους τα Μέρη ή οι εργολάβοι, υπεργολάβοι ή τα νομικά πρόσωπα δημοσίου ή ιδιωτικού δικαίου, που είναι εξουσιοδοτημένα να χειρίζονται και αποθηκεύουν Διαβαθμισμένες Πληροφορίες.

Άρθρο 2
Ορισμοί

Για τους σκοπούς της παρούσας Συμφωνίας:

«Παραβίαση Ασφαλείας» σημαίνει πράξη ή παράλειψη η οποία αντιβαίνει στην παρούσα Συμφωνία ή στην εθνική νομοθεσία των Μερών και το αποτέλεσμα της οποίας ενδέχεται να οδηγήσει στην γνωστοποίηση, απώλεια, καταστροφή, παράνομη χρήση ή οποιαδήποτε άλλη διαρροή των Διαβαθμισμένων Πληροφοριών,

«Διαβαθμισμένη Σύμβαση» σημαίνει κάθε συμφωνία μεταξύ δύο ή περισσοτέρων Εργολάβων ή υπεργολάβων και η εκτέλεση της οποίας απαιτεί ή περιλαμβάνει πρόσβαση ή στη δημιουργία, Διαβαθμισμένων Πληροφοριών.

«Διαβαθμισμένες Πληροφορίες» σημαίνει κάθε πληροφορία, ανεξαρτήτως τύπου ή φύσεως, η οποία χρήζει προστασίας από μη εξουσιοδοτημένη πρόσβαση ή χειρισμό και διαβαθμίστηκε με κάποιο επίπεδο διαβάθμισης ασφαλείας, σύμφωνα με την εθνική νομοθεσία των Μερών,

«Αρμόδια Αρχή Ασφαλείας» σημαίνει οποιαδήποτε Αρμόδια Αρχή των Μερών εκτός των Εθνικών Αρχών Ασφαλείας, η οποία σύμφωνα με την εθνική νομοθεσία των Μερών, είναι υπεύθυνη για την εφαρμογή της παρούσας Συμφωνίας,

«Εργολάβος» σημαίνει το φυσικό ή νομικό πρόσωπο που έχει τη νομική ικανότητα ανάληψης συμβάσεων,

«Εξουσιοδότηση Ασφαλείας Φορέα» σημαίνει τη θετική απόφαση της Αρμόδιας Αρχής Ασφαλείας, με την οποία επιβεβαιώνεται ότι, το νομικό πρόσωπο έχει την φυσική και οργανωτική ικανότητα να χειρίζεται και να αποθηκεύει Διαβαθμισμένες Πληροφορίες σύμφωνα με την αντίστοιχη εθνική νομοθεσία των Μερών,

«Εθνική Αρχή Ασφαλείας» σημαίνει την κρατική αρχή κάθε Μέρους, η οποία σύμφωνα με την εθνική του νομοθεσία είναι υπεύθυνη για την γενική εφαρμογή και εποπτεία της παρούσας Συμφωνίας. Οι αντίστοιχες αρχές των Μερών αναφέρονται στο Άρθρο 4, Παράγραφος 1 της παρούσας Συμφωνίας.

«Ανάγκη για γνώση» σημαίνει την ανάγκη πρόσβασης σε συγκεκριμένες Διαβαθμισμένες Πληροφορίες στα πλαίσια συγκεκριμένης επίσημης θέσης και για την εκτέλεση συγκεκριμένης εργασίας.

«Μέρος Αποστολέας» σημαίνει το Μέρος το οποίο παρέχει Διαβαθμισμένες Πληροφορίες στο Μέρος Παραλήπτη.

«Εξουσιοδότηση Ασφαλείας Προσωπικού» σημαίνει τη θετική απόφαση της Αρμόδιας Αρχής Ασφαλείας, σύμφωνα με την αντίστοιχη εθνική νομοθεσία των Μερών, κατά την οποία το πρόσωπο δικαιούται να έχει πρόσβαση σε Διαβαθμισμένες Πληροφορίες και να τις χειρίζεται έως ένα συγκεκριμένο επίπεδο,

«Μέρος Παραλήπτης» σημαίνει το Μέρος στο οποίο διαβιβάζονται

Διαβαθμισμένες Πληροφορίες,

«Τρίτο Μέρος» σημαίνει το κράτος, τον οργανισμό, το νομικό ή φυσικό πρόσωπο το οποίο δεν είναι συμβαλλόμενο μέρος στην παρούσα Συμφωνία.

Άρθρο 3
Επίπεδα Διαβάθμισης Ασφαλείας

Τα Μέρη συμφωνούν ότι τα ακόλουθα επίπεδα διαβάθμισης ασφαλείας και διαβαθμίσεις ισοδυναμούν και αντιστοιχούν στα επίπεδα διαβάθμισης ασφαλείας τα οποία ορίζονται από την εθνική τους νομοθεσία:

SEGRETISSIMO	ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ	TOP SECRET
SEGRETO	ΑΠΟΡΡΗΤΟ	SECRET
RISERVATISSIMO	ΕΜΠΙΣΤΕΥΤΙΚΟ	CONFIDENTIAL
RISERVATO	ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ	RESTRICTED

Άρθρο 4
Αρμόδιες Αρχές Ασφαλείας

1. Οι Εθνικές Αρχές Ασφαλείας των Μερών είναι:

   Για την Ιταλική Δημοκρατία:
   Presidenza del Consiglio dei Ministri – Dipartimento delle Informazioni per la Sicurezza (DIS) – UCSe

   Για την Κυπριακή Δημοκρατία:
   Εθνική Αρχή Ασφαλείας
   Υπουργείο Άμυνας της Κυπριακής Δημοκρατίας

2. Τα Μέρη θα αλληλοενημερώνονται μέσω της διπλωματικής οδού για τυχόν αλλαγές που αφορούν στις Εθνικές Αρχές Ασφαλείας.

3. Κατόπιν αιτήματος, οι Εθνικές Αρχές Ασφαλείας θα αλληλοενημερώνονται σχετικά με άλλες Αρμόδιες Αρχές.

4. Οι Εθνικές Αρχές Ασφαλείας θα αλληλοενημερώνονται για την αντίστοιχη εθνική νομοθεσία περί Διαβαθμισμένων Πληροφοριών και για τυχόν σημαντικές τροποποιήσεις σε αυτή και θα ανταλλάσσουν πληροφορίες σχετικά με τα πρότυπα, τις διαδικασίες και πρακτικές που αφορούν στην προστασία Διαβαθμισμένων Πληροφοριών.

Άρθρο 5
Μέτρα Προστασίας και Πρόσβαση σε Διαβαθμισμένες Πληροφορίες

1. Σύμφωνα με την εθνική τους νομοθεσία, τα Μέρη λαμβάνουν όλα τα κατάλληλα μέτρα για την προστασία Διαβαθμισμένων Πληροφοριών τις οποίες παράγουν ή ανταλλάσσουν βάσει της παρούσας Συμφωνίας. Οι Διαβαθμισμένες Πληροφορίες που παράγονται ή παρέχονται βάσει της παρούσας Συμφωνίας θα διαβαθμίζονται με το ίδιο τουλάχιστον επίπεδο ασφαλείας, όπως προβλέπεται για τις εθνικές Διαβαθμισμένες Πληροφορίες του αντίστοιχου επιπέδου διαβάθμισης ασφαλείας σύμφωνα με το Άρθρο 3.

2. Το Μέρος Αποστολέας ενημερώνει:

   α) το Μέρος Παραλήπτη για τυχόν προϋποθέσεις υποβολής ή περιορισμούς χρήσης των Διαβαθμισμένων Πληροφοριών,

   β) γραπτώς το Μέρος Παραλήπτη για τυχόν αλλαγή στο επίπεδο διαβάθμισης ασφαλείας των διαβιβασθέντων Διαβαθμισμένων Πληροφοριών.

3. Η πρόσβαση σε Διαβαθμισμένες Πληροφορίες επιπέδου RISERVATISSIMO/ ΕΜΠΙΣΤΕΥΤΙΚΟ/ CONFIDENTIAL ή υψηλότερου περιορίζεται σε φυσικά και νομικά πρόσωπα τα οποία έχουν εξασφαλίσει κατάλληλη Εξουσιοδότηση Ασφαλείας Προσωπικού βάσει της αρχής της Ανάγκης για γνώση σύμφωνα με την εθνική νομοθεσία των Μερών.

4. Δεν απαιτείται Εξουσιοδότηση Ασφαλείας Προσωπικού για πρόσβαση σε Διαβαθμισμένες Πληροφορίες επιπέδου RISERVATO/ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ / RESTRICTED. Η πρόσβαση αυτή περιορίζεται σε φυσικά πρόσωπα βάσει της αρχής της Ανάγκης για γνώση, και τα οποία έχουν ενημερωθεί καταλλήλως για τις ευθύνες τους και τις υποχρεώσεις τους σχετικά με την προστασία τέτοιων Διαβαθμισμένων Πληροφοριών.

5. Στο πλαίσιο της παρούσας Συμφωνίας, κάθε Μέρος αναγνωρίζει την Εξουσιοδότηση Ασφαλείας Προσωπικού και Φορέα, η οποία παρέχεται σύμφωνα με την εθνική νομοθεσία του κράτους του άλλου Μέρους. Οι εξουσιοδοτήσεις ασφαλείας θα είναι ισοδύναμες με τις διαβαθμίσεις που

αναφέρονται στο Άρθρο 3.

6. Οι Εθνικές Αρχές Ασφαλείας, κατόπιν αιτήματος και σύμφωνα με την αντίστοιχη εθνική νομοθεσία τους, αλληλοβοηθούνται στη διεξαγωγή των διαδικασιών ελέγχου ασφαλείας για την εφαρμογή της παρούσας Συμφωνίας.

7. Στο πλαίσιο της παρούσας Συμφωνίας, οι Αρμόδιες Αρχές των Μερών αλληλοενημερώνονται χωρίς καθυστέρηση σχετικά με τυχόν αλλαγές των Εξουσιοδοτήσεων Ασφαλείας Προσωπικού και Φορέα, και πιο συγκεκριμένα όταν πρόκειται για την απόσυρση ή την υποβάθμισή τους.

8. Το Μέρος Παραλήπτης:

   α) υποβάλλει Διαβαθμισμένες Πληροφορίες σε τυχόν Τρίτο Πρόσωπο μόνο μετά την παραλαβή της προηγούμενης γραπτής συγκατάθεσης του Μέρους Αποστολέα,

   β) διαβαθμίζει την παραληφθείσα Διαβαθμισμένη πληροφορία σύμφωνα με το Άρθρο 3,

   γ) χρησιμοποιεί Διαβαθμισμένες Πληροφορίες μόνο για τους σκοπούς για τους οποίους προβλέπονται.

Άρθρο 6
Διαβίβαση Διαβαθμισμένων Πληροφοριών

1. Διαβαθμισμένες Πληροφορίες επιπέδου SEGRETISSIMO/ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ/ TOP SECRET διαβιβάζονται μέσω Κυβερνητικής οδού σύμφωνα με την εθνική νομοθεσία των Μερών. Ως ελάχιστο επίπεδο οι εν λόγω Διαβαθμισμένες Πληροφορίες θα μεταφέρονται από Κυβερνητικό ταχυμεταφορέα και υπό τον αποκλειστικό έλεγχο αυτού, ο οποίος έχει εξασφαλίσει Εξουσιοδότηση Ασφαλείας Προσωπικού επιπέδου SEGRETISSIMO / ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ / TOP SECRET. Το Μέρος Παραλήπτης επιβεβαιώνει γραπτώς τη λήψη Διαβαθμισμένων Πληροφοριών επιπέδου SEGRETISSIMO / ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ / TOP SECRET.

2. Διαβαθμισμένες Πληροφορίες επιπέδου SEGRETO/ΑΠΟΡΡΗΤΟ/ SECRET ή RISERVATISSIMO/ΕΜΠΙΣΤΕΥΤΙΚΟ/CONFIDENTIAL διαβιβάζονται μέσω Κυβερνητικής οδού σύμφωνα με την εθνική νομοθεσία των Μερών, ή μέσω άλλης ασφαλούς οδού η οποία έχει εγκριθεί από της Αρχές Ασφαλείας και των δύο Μερών. Το Μέρος Παραλήπτης επιβεβαιώνει γραπτώς τη λήψη Διαβαθμισμένων Πληροφοριών επιπέδου SEGRETO/ΑΠΟΡΡΗΤΟ/ SECRET και RISERVATISSIMO /ΕΜΠΙΣΤΕΥΤΙΚΟ /CONFIDENTIAL.

3. Διαβαθμισμένες Πληροφορίες επιπέδου RISERVATO/ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ/RESTRICTED διαβιβάζονται μέσω ασφαλούς οδού σύμφωνα με την εθνική νομοθεσία των Μερών.

4. Οι διαδικασίες για μεταφορά μεγάλου φορτίου Διαβαθμισμένων Πληροφοριών συμφωνούνται αμοιβαία και αξιολογούνται κατά περίπτωση από την Εθνική Αρχή Ασφαλείας των δύο Μερών.

5. Διαβαθμισμένες Πληροφορίες επιπέδου SEGRETO/ΑΠΟΡΡΗΤΟ/ SECRET, RISERVATISSIMO/ΕΜΠΙΣΤΕΥΤΙΚΟ/ CONFIDENTIAL και RISERVATO/ ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ/ RESTRICTED, οι οποίες πρόκειται να διαβιβαστούν ηλεκτρονικά μεταξύ των Μερών, δεν αποστέλλονται ακρυπτογράφητες. Η ηλεκτρονική διαβίβαση των συγκεκριμένων Διαβαθμισμένων Πληροφοριών διεξάγεται μέσω πιστοποιημένων κρυπτογραφικών μέσων τα οποία εγκρίνονται αμοιβαία από τις Εθνικές Αρχές Ασφαλείας.

6. Τα κύρια σημεία εισόδου και εξόδου Διαβαθμισμένων Πληροφοριών τις οποίες ανταλλάσσουν τα Μέρη στο πλαίσιο της παρούσας Συμφωνίας είναι:

   Για την Ιταλική Δημοκρατία:

   α) Όπως προβλέπεται από την εθνική της νομοθεσία.

   β) Η Εθνική Αρχή Ασφαλείας αναλαμβάνει την υποχρέωση να παράσχει στο Υπουργείο Εξωτερικών της Κυπριακής Δημοκρατίας επικαιροποιημένο κατάλογο με τα σημεία ασφαλείας εισόδου και εξόδου Διαβαθμισμένων Πληροφοριών, τα οποία βάσει της ιταλικής νομοθεσίας θεωρούνται ως «δημόσια».

   Για την Κυπριακή Δημοκρατία:
   Κεντρική Γραμματεία ΑΚΡΩΣ ΑΠΟΡΡΗΤΩΝ του Υπουργείο Εξωτερικών.

Άρθρο 7
Αναπαραγωγή και Μετάφραση Διαβαθμισμένων Πληροφοριών

1. Οι Διαβαθμισμένες Πληροφορίες μεταφράζονται και αναπαράγονται σύμφωνα με την εθνική νομοθεσία του Μέρους Παραλήπτη και υπό τις ακόλουθες διαδικασίες:

   α) οι μεταφράσεις και οι αναπαραγωγές διαβαθμίζονται και προστατεύονται όπως και οι πρωτότυπες Διαβαθμισμένες Πληροφορίες;

β) οι μεταφράσεις και ο αριθμός των αντιγράφων περιορίζονται στον αριθμό που απαιτείται για επίσημους σκοπούς;

γ) οι μεταφράσεις φέρουν κατάλληλη σημείωση στη γλώσσα μετάφρασης, υποδεικνύοντας ότι περιέχουν Διαβαθμισμένες Πληροφορίες που λήφθηκαν από το Μέρος Αποστολέα.

2. Οι Διαβαθμισμένες Πληροφορίες επιπέδου SEGRETO/ ΑΠΟΡΡΗΤΟ/ SECRET και άνω, μεταφράζονται ή αναπαράγονται μόνο κατόπιν της γραπτής συγκατάθεσης του Μέρους Αποστολέα.

Άρθρο 8
Καταστροφή Διαβαθμισμένων Πληροφοριών

1. Οι Διαβαθμισμένες Πληροφορίες καταστρέφονται ώστε να αποφευχθεί η μερική ή ολική ανακατασκευή τους.

2. Οι Διαβαθμισμένες Πληροφορίες επιπέδου έως SEGRETO/ΑΠΟΡΡΗΤΟ/ SECRET καταστρέφονται σύμφωνα με την εθνική νομοθεσία των Μερών.

3. Οι Διαβαθμισμένες Πληροφορίες επιπέδου SEGRETISSIMO/ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ/ TOP SECRET δεν καταστρέφονται. Επιστρέφονται στην Αρμόδια Αρχή του Μέρους Αποστολέα

4. Συντάσσεται έκθεση για την καταστροφή των Διαβαθμισμένων Πληροφοριών και η μετάφρασή της στην αγγλική γλώσσα αποστέλλεται στην Αρχή Ασφαλείας του Μέρους Αποστολέα.

5. Σε περίπτωση κατάστασης κρίσης κατά την οποία δεν είναι δυνατή η προστασία ή η επιστροφή Διαβαθμισμένων Πληροφοριών, αυτές καταστρέφονται αμέσως. Το Μέρος Παραλήπτης ενημερώνει την Αρχή Ασφαλείας του Μέρους Αποστολέα σχετικά με την εν λόγω καταστροφή το συντομότερο δυνατόν.

Άρθρο 9
Διαβαθμισμένες Συμβάσεις

1. Η Εθνική Αρχή Ασφαλείας του ενός Μέρους παρέχει στην Εθνική Αρχή

Ασφαλείας του άλλου Μέρους, γραπτή εγγύηση ότι ο εργολάβος ή υπεργολάβος που επιθυμεί να αναλάβει διαβαθμισμένη σύμβαση επιπέδου RISERVATISSIMO/ ΕΜΠΙΣΤΕΥΤΙΚΟ/ CONFIDENTIAL και SEGRETO/ ΑΠΟΡΡΗΤΟ/ SECRET με αυτό το άλλο Μέρος, είναι κάτοχος ή βρίσκεται στη διαδικασία για την εξασφάλιση Εξουσιοδότησης Ασφαλείας Φορέα με το αντίστοιχο επίπεδο διαβάθμισης ασφαλείας.

2. Κάθε Διαβαθμισμένη Σύμβαση που συνάπτεται σύμφωνα με την παρούσα Συμφωνία περιλαμβάνει:

α) δέσμευση συμμόρφωσης με τις πρόνοιες της παρούσας Συμφωνίας;

β) δέσμευση του Εργολάβου ή του υπεργολάβου, με την οποία διασφαλίζεται ότι οι εγκαταστάσεις τους τηρούν τις απαραίτητες προϋποθέσεις για τον χειρισμό και την αποθήκευση Διαβαθμισμένων Πληροφοριών με το αντίστοιχο επίπεδο διαβάθμισης ασφαλείας;

γ) δέσμευση του Εργολάβου ή του υπεργολάβου, με την οποία διασφαλίζεται ότι τα άτομα που εκτελούν καθήκοντα τα οποία απαιτούν πρόσβαση σε Διαβαθμισμένες Πληροφορίες είναι δεόντως εξουσιοδοτημένα, σύμφωνα με την εθνική νομοθεσία, να έχουν πρόσβαση σε Διαβαθμισμένες Πληροφορίες με το αντίστοιχο επίπεδο διαβάθμισης ασφαλείας και ότι ενημερώνονται τακτικά για θέματα ασφαλείας;

δ) κατάλογο με τις Διαβαθμισμένες Πληροφορίες και τους χώρους χειρισμού και αποθήκευσης των Διαβαθμισμένων Πληροφοριών;

ε) δέσμευση κοινοποίησης τυχόν αλλαγών στο επίπεδο διαβάθμισης ασφαλείας των Διαβαθμισμένων Πληροφοριών;

στ) τις διαδικασίες διαβίβασης Διαβαθμισμένων Πληροφοριών;

ζ) δέσμευση του Εργολάβου ή του υπεργολάβου ότι θα ενημερώσει την Εθνική Αρχή Ασφαλείας του για τυχόν πραγματική ή ενδεχόμενη Παραβίαση Ασφαλείας;

η) δέσμευση του Εργολάβου ή του υπεργολάβου ότι θα προωθήσει αντίγραφο της Διαβαθμισμένης Σύμβασης στην Εθνική Αρχή Ασφαλείας και των δύο Μερών.

3. Δεν απαιτείται Εξουσιοδότηση Ασφαλείας Φορέα ούτε και Εξουσιοδότηση Ασφαλείας Προσωπικού για Διαβαθμισμένες Συμβάσεις που περιορίζονται σε

Διαβαθμισμένες Πληροφορίες επιπέδου RISERVATO / ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ / RESTRICTED. Οι εν λόγω Διαβαθμισμένες Συμβάσεις περιέχουν κατάλληλη ρήτρα απαίτησης ασφαλείας, η οποία ορίζει την ελάχιστη απαίτηση ασφαλείας που πρέπει να εφαρμοστεί από τον Εργολάβο σε Διαβαθμισμένες Πληροφορίες που παράγονται και/ή παρέχονται ως αποτέλεσμα της Σύμβασης. Η ρήτρα ασφαλείας πρέπει να περιλαμβάνει πρόνοια αναφορικά με τον διορισμό, από τον Εργολάβο, προσώπου το οποίο θα έχει την πλήρη ευθύνη για την προστασία Διαβαθμισμένων Πληροφοριών επιπέδου RISERVATO / ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ/ RESTRICTED. Αντίγραφο της πρόνοιας απαίτησης ασφαλείας παρέχεται στην Εθνική Αρχή Ασφαλείας μόνο εφόσον ζητηθεί.

4. Για σκοπούς βιομηχανικής ασφαλείας μόνο, βάσει της ιταλικής νομοθεσίας τα σημεία εισόδου και εξόδου Διαβαθμισμένων Πληροφοριών, υπό την έννοια της παραγράφου 6, του Άρθρου 6 της παρούσας Συμφωνίας, είναι τα όργανα ασφαλείας των Εργολάβων ή υπεργολάβων που διαθέτουν Εξουσιοδότηση Ασφαλείας Φορέα.

Άρθρο 10
Διαβαθμισμένες Επισκέψεις

1. Οι επίσημες κυβερνητικές επισκέψεις που συνεπάγονται πρόσβαση σε Διαβαθμισμένες Πληροφορίες επιπέδου SEGRETISSIMO / ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ / TOP SECRET, SEGRETO / ΑΠΟΡΡΗΤΟ / SECRET και RISERVATISSIMO / ΕΜΠΙΣΤΕΥΤΙΚΟ / CONFIDENTIAL πρέπει να διεξάγονται κατόπιν υποβολής Εξουσιοδότησης Ασφαλείας Προσωπικού πριν από την επίσκεψη.

2. Για τους σκοπούς της παρούσας Συμφωνίας, όλα τα υπόλοιπα είδη επισκέψεων, τα οποία δεν προβλέπονται από την παράγραφο 1 και συνεπάγονται πρόσβαση σε Διαβαθμισμένες Πληροφορίες επιπέδου RISERVATISSIMO / ΕΜΠΙΣΤΕΥΤΙΚΟ / CONFIDENTIAL και SEGRETO/ ΑΠΟΡΡΗΤΟ/ SECRET, υπόκεινται στην εκ των προτέρων γραπτή έγκριση της Εθνικής Αρχής Ασφαλείας του Μέρους υποδοχής.

3. Η Εθνική Αρχή Ασφαλείας του Μέρους υποδοχής θα πρέπει να λάβει αίτηση επίσκεψης τουλάχιστον 20 (είκοσι) ημέρες νωρίτερα.

4. Σε έκτακτες περιπτώσεις η αίτηση επίσκεψης μπορεί να διαβιβαστεί εντός συντομότερης προθεσμίας.

5. Η αίτηση επίσκεψης περιλαμβάνει:

   α) ονοματεπώνυμο του επισκέπτη, τόπο και ημερομηνία γέννησης, υπηκοότητα και αριθμό διαβατηρίου ή ταυτότητας;

β) επωνυμία του νομικού προσώπου το οποίο εκπροσωπεί ο επισκέπτης και τη θέση του επισκέπτη στο νομικό πρόσωπο;

γ) επωνυμία, διεύθυνση και στοιχεία επικοινωνίας του νομικού προσώπου και των εγκαταστάσεων που πρόκειται να δεχθούν την επίσκεψη;

δ) επιβεβαίωση της Εξουσιοδότησης Ασφαλείας Προσωπικού του επισκέπτη, της εγκυρότητάς του και του επιπέδου του;

ε) σκοπό και λόγους της επίσκεψης, καθώς και το υψηλότερο επίπεδο διαβάθμισης ασφαλείας των συναφών Διαβαθμισμένων Πληροφοριών;

στ) αναμενόμενη ημερομηνία και διάρκεια της επίσκεψης. Σε περίπτωση επαναλαμβανόμενων επισκέψεων, αναφέρεται η συνολική διάρκεια των επισκέψεων;

ζ) ημερομηνία, υπογραφή και επίσημη σφραγίδα του εξουσιοδοτημένου οργάνου ασφαλείας.

6. Μόλις εγκριθεί η επίσκεψη, η Εθνική Αρχή Ασφαλείας του Μέρους υποδοχής παρέχει αντίγραφο της αίτησης επίσκεψης στο λειτουργό ασφαλείας του νομικού προσώπου που πρόκειται να δεχτεί την επίσκεψη.

7. Η ισχύς της έγκρισης επίσκεψης δεν υπερβαίνει το ένα έτος.

8. Οι Εθνικές Αρχές Ασφαλείας των Μερών δύνανται να καταρτίσουν καταλόγους με φυσικά πρόσωπα τα οποία είναι εξουσιοδοτημένα να κάνουν επαναλαμβανόμενες επισκέψεις. Αυτοί οι κατάλογοι ισχύουν για αρχική περίοδο δώδεκα (12) μηνών. Οι όροι των αντίστοιχων επισκέψεων θα καθορίζονται από τα αρμόδια άτομα του νομικού προσώπου που πρόκειται να δεχτεί την επίσκεψη, σύμφωνα με τους όρους και τις προϋποθέσεις που θα συμφωνηθούν.

Άρθρο 11
Παραβίαση Ασφαλείας

1. Σε περίπτωση Παραβίασης Ασφαλείας, η Εθνική Αρχή Ασφαλείας του Μέρους Παραλήπτη ενημερώνει την Εθνική Αρχή Ασφαλείας του Μέρους Αποστολέα, το συντομότερο δυνατόν, και ξεκινά την κατάλληλη έρευνα.

2. Εάν η Παραβίαση Ασφαλείας επέλθει σε τρίτο κράτος, η Εθνική Αρχή Ασφαλείας του Μέρους το οποίο αποδέσμευσε τις πληροφορίες σε τρίτο κράτος λαμβάνει όλα τα απαραίτητα μέτρα για να διασφαλίσει ότι οι ενέργειες που περιγράφονται στην Παράγραφο 1 έχουν τεθεί σε εφαρμογή.

3. Το Μέρος Αποστολέας, κατόπιν αιτήματος, συνεργάζεται στην έρευνα σύμφωνα με την παράγραφο 1.

4. Το Μέρος Αποστολέας ενημερώνεται για τα αποτελέσματα της έρευνας και λαμβάνει την τελική έκθεση για τις αιτίες και την έκταση της ζημιάς.

Άρθρο 12
Έξοδα

1. Δεν απαιτούνται έξοδα για την εφαρμογή της παρούσας Συμφωνίας.

2. Με την επιφύλαξη της παραγράφου 1, κάθε Μέρος αναλαμβάνει τα πιθανά του απροσδόκητα έξοδα που προκύπτουν κατά την εφαρμογή και εποπτεία της παρούσας Συμφωνίας.

Άρθρο 13
Διευθέτηση Διαφορών

Τυχόν διαφορές που προκύπτουν από την ερμηνεία ή εφαρμογή της παρούσας Συμφωνίας, διευθετούνται με διαπραγματεύσεις μεταξύ των Μερών.

Άρθρο 14
Τελικές Πρόνοιες

1 Η παρούσα Συμφωνία συνάπτεται για απεριόριστο χρονικό διάστημα και τίθεται σε ισχύ την πρώτη ημέρα του δεύτερου μήνα μετά την ημερομηνία λήψης της τελευταίας γραπτής ειδοποίησης με την οποία τα Μέρη ανακοινώνουν το ένα στο άλλο, μέσω της διπλωματικής οδού, ότι έχουν εκπληρωθεί όλες οι αναγκαίες εθνικές νομικές προϋποθέσεις που απαιτούνται για την έναρξη ισχύος της παρούσας Συμφωνίας.

2. Η παρούσα Συμφωνία δύναται να τροποποιείται ανά πάσα στιγμή, κατόπιν αμοιβαίας γραπτής έγκρισης των Μερών. Οι τροποποιήσεις τίθενται σε ισχύ σύμφωνα με την Παράγραφο 1.

3. Κάθε Μέρος δύναται, ανά πάσα στιγμή, να καταγγείλει τη Συμφωνία με γραπτή ειδοποίηση προς το άλλο Μέρος, μέσω της διπλωματικής οδού. Στην περίπτωση αυτή, η λήξη της Συμφωνίας θα ισχύει έξι μήνες μετά την ημερομηνία λήψης της αντίστοιχης ανακοίνωσης.

4. Παρά την καταγγελία της παρούσας Συμφωνίας, τα Μέρη διασφαλίζουν ώστε όλες οι Διαβαθμισμένες Πληροφορίες θα συνεχίσουν να προστατεύονται έως ότου το Μέρος Αποστολέας απαλλάξει το Μέρος Παραλήπτη από τις υποχρεώσεις του.

Συντάχθηκε στην Λευκωσία στις 31 Ιουλίου 2017 σε δύο πρωτότυπα σετ αντιγράφων, στην Ιταλική, Ελληνική και Αγγλική γλώσσα, και όλα τα κείμενα είναι εξίσου αυθεντικά. Σε περίπτωση διαφωνίας στην ερμηνεία, το Αγγλικό κείμενο υπερισχύει.

Για την Κυβέρνηση της Ιταλικής Δημοκρατίας	**Για την Κυβέρνηση της Κυπριακής Δημοκρατίας**
.....	.....

AGREEMENT BETWEEN THE GOVERNMENT OF THE ITALIAN REPUBLIC AND THE GOVERNMENT OF THE REPUBLIC OF CYPRUS ON THE EXCHANGE AND MUTUAL PROTECTION OF CLASSIFIED INFORMATION

The Government of the Italian Republic
and
the Government of the Republic of Cyprus

(hereinafter referred to as "the Parties"),

Recognizing the need to set rules on protection of Classified Information mutually exchanged in the interest of national security within the scope of political, military, economical, legal, scientific and technological or any other cooperation, as well as Classified Information generated in the process of such cooperation;

Intending to ensure the mutual protection of all Classified Information, which has been classified by one Party and transferred to the other Party or jointly generated in the course of cooperation between the Parties;

Desiring to create a set of rules on the mutual protection of Classified Information exchanged between the Parties;

Considering the mutual interests in the protection of Classified Information, in accordance with the legislation of the Parties;

Have agreed as follows:

Article 1
Objective

The objective of this Agreement is to ensure the protection of Classified Information that is generated or mutually exchanged between the Parties or contractors, sub-contractors or any other public or private legal person authorised to handle and store Classified Information.

Article 2
Definitions

For the purposes of this Agreement:

"Breach of Security" means an act or an omission which is contrary to this Agreement or to the national legislation of the Parties, the result of which may

lead to disclosure, loss, destruction, misappropriation or any other type of compromise of Classified Information.

"**Classified Contract**" means an agreement between two or more Contractors or sub-contractors, which contains or involves access to, or the creation of Classified Information.

"**Classified Information**" means any information, regardless of its form or nature, which requires protection against unauthorised access or manipulation and for which a security classification level has been assigned, in accordance with the national legislation of the Parties.

"**Competent Security Authority**" means any competent authority of the Parties other than the NSA's that according to its national legislation, is responsible for the implementation of this Agreement.

"**Contractor**" means a legal person having the legal capacity to conclude or undertake contracts.

"**Facility Security Clearance**" means the positive decision by the Security Authority confirming that the legal person has the physical and organizational capability to handle and store Classified Information in accordance with the respective national legislation of both Parties.

"**National Security Authority**" means the state authority of each Party, which in accordance with its national legislation is responsible for the general implementation and supervision of this Agreement; the respective authorities of the Parties are referred to in Article 4 paragraph 1 of this Agreement.

"**Need-to-know**" means the principle whereby access to specific Classified Information is granted exclusively in the scope of a given official position and for the performance of a specific task.

"**Providing Party**" means the Party that provides classified information to the Receiving Party.

"**Personnel Security Clearance**" means the positive decision by the Security Authority confirming, in accordance with the respective national legislation of the Parties, that a person is authorized to have access to and handle Classified Information up to a specific level.

"**Receiving Party**" means the Party to which Classified Information is transmitted.

"**Third Party**" means any State, organization, legal or natural person, which is

not a party to this Agreement.

Article 3
Security Classification Levels

The Parties agree that the following security classification levels and markings are equivalent and correspond to the security classification levels specified in their national legislation:

SEGRETISSIMO	ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ	TOP SECRET
SEGRETO	ΑΠΟΡΡΗΤΟ	SECRET
RISERVATISSIMO	ΕΜΠΙΣΤΕΥΤΙΚΟ	CONFIDENTIAL
RISERVATO	ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ	RESTRICTED

Article 4
Security Authorities

1. The National Security Authorities of the Parties are:

For the Italian Republic:
Presidenza del Consiglio dei Ministri – Dipartimento delle Informazioni per la Sicurezza (DIS) – UCSe

For the Republic of Cyprus:
National Security Authority
Ministry of Defence of the Republic of Cyprus

2. The Parties shall inform each other through diplomatic channels of any modification of the National Security Authorities.

3. Upon request the National Security Authorities shall notify each about other Security Authorities.

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

Information.

Article 5
Protection Measures and Access to Classified Information

1. In accordance with their national legislation, the Parties shall take all necessary measures for the protection of Classified Information that is created or exchanged under this Agreement. The Parties shall afford to Classified Information created and/or provided under this Agreement the same level of protection as they would to their own Classified Information at the security classification level, as set out in Article 3.

2. The Providing Party shall inform:

a) the Receiving Party of any conditions of release or limitations on the use of the Classified Information;

b) the Receiving Party in writing about any change of the security classification level of the transmitted Classified Information.

3. Access to Classified Information at RISERVATISSIMO / ΕΜΠΙΣΤΕΥΤΙΚΟ /CONFIDENTIAL level and above shall be limited to natural and legal persons holding an adequate security clearance on a Need-to-know basis in accordance to the national legislation of the Parties.

4. A Personnel Security Clearance is not required for access to Classified Information marked RISERVATO / ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ / RESTRICTED. Such access shall be limited to physical persons on a Need-to-know basis and who have been appropriately briefed on their responsibilities and obligations to protect such Classified Information.

5. Within the scope of this Agreement, each Party shall recognise the Personnel Security Clearances and Facility Security Clearances granted in accordance with the national legislation of the other Party. The security clearances shall be equivalent to the levels provided in Article 3.

6. The National Security Authorities shall, in accordance with their respective national legislation, assist each other upon request at carrying out vetting procedures necessary for the application of this Agreement.

7. Within the scope of this Agreement, the Security Authorities of the Parties shall inform each other without delay about any alteration with regard to Personnel and Facility Security Clearances, in particular about their

withdrawal or downgrading.

8. The Receiving Party shall:

a) release Classified Information to any Third Party only upon receipt of the prior written consent of the Providing Party.

b) mark the received Classified Information in accordance with Article 3;

c) use Classified Information solely for the purposes which it has been provided for.

Article 6
Transmission of Classified Information

1. Classified Information marked as SEGRETISSIMO / ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ /TOP SECRET shall be transmitted through Government to Government channels in accordance with the national legislations 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 Personnel Security Clearance to SEGRETISSIMO / ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ /TOP SECRET level. The Receiving Party shall confirm the receipt of SEGRETISSIMO / ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ /TOP SECRET Classified Information in writing.

2. Classified Information marked as SEGRETO / ΑΠΟΡΡΗΤΟ /SECRET or RISERVATISSIMO / ΕΜΠΙΣΤΕΥΤΙΚΟ /CONFIDENTIAL shall be transmitted through Government to Government channels in accordance with the national legislation of the Parties, or through other secure channels mutually approved by the Security Authorities of both Parties. The Receiving Party shall confirm the receipt of SEGRETO / ΑΠΟΡΡΗΤΟ /SECRET and / ΕΜΠΙΣΤΕΥΤΙΚΟ RISERVATISSIMO/CONFIDENTIAL Classified Information in writing.

3. Classified Information marked as RISERVATO / ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ /RESTRICTED shall be transmitted through secure channels in accordance to the national legislation of the Parties.

4. The procedures for the carriage of large consignments containing Classified Information shall be jointly agreed and evaluated, on a case-by-case basis, by the National Security Authority of both Parties.

5. If Classified Information marked as SEGRETO / ΑΠΟΡΡΗΤΟ /SECRET, RISERVATISSIMO / ΕΜΠΙΣΤΕΥΤΙΚΟ /CONFIDENTIAL and RISERVATO / ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ /RESTRICTED is to be transmitted electronically between the Parties, it shall not be sent in clear text. Electronic transmission

of these specific classification levels shall be carried out through certified cryptographic means mutually approved by the National Security Authorities.

6. The main points of entry and exit for the Classified Information exchange under this Agreement shall be:

For the Italian Republic:
a) As provided by its national legislation.

b) The National Security Authority undertakes the responsibility to provide updated list of the security points of entry and exit of entities considered as 'public' under Italian legislation, for the classified information, to the Ministry of Foreign Affairs, of the Republic of Cyprus.

For the Republic of Cyprus:
The Central TOP SECRET Registry at the Ministry of Foreign Affairs.

Article 7
Reproduction and Translation of Classified Information

1. Translations and reproductions of Classified Information shall be made in accordance to the national legislation of the Receiving Party and the following procedures:

a) the translations and the reproductions shall be marked and protected as the original Classified Information;

b) the translations and the number of copies shall be limited to that required for official purposes;

c) the translations shall bear an appropriate annotation in the language of the translation indicating that it contains Classified Information received from the Providing Party.

2. Classified Information marked as SEGRETO / ΑΠΟΡΡΗΤΟ /SECRET or above level shall be translated or reproduced only upon the prior written consent of the Providing Party.

Article 8
Destruction of Classified Information

1. Classified Information shall be destroyed in a way that prevents its partial or total reconstruction.

2. Classified Information marked up to SEGRETO / ΑΠΟΡΡΗΤΟ /SECRET shall be destroyed in accordance with the national legislation of the Parties.

3. Classified Information marked as SEGRETISSIMO / ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ /TOP SECRET shall not be destroyed. It shall be returned to the Security Authority of the Providing Party.

4. A report on destruction of Classified Information shall be made and its translation in English shall be delivered to the Security Authority of the Providing Party.

5. 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 Providing Party about this destruction as soon as possible.

Article 9
Classified Contracts

1. The National Security Authority of a Party shall provide to the National Security Authority of the other Party prior written assurance that a contractor or a sub-contractor, wishing to undertake a classified contract marked as RISERVATISSIMO / ΕΜΠΙΣΤΕΥΤΙΚΟ / CONFIDENTIAL and SEGRETO / ΑΠΟΡΡΗΤΟ /SECRET level with such other Party, holds or is in the process of obtaining a Facility Security Clearance of the appropriate security classification level.

2. Each Classified Contract in accordance to this Agreement shall include:

a) a commitment to comply with the provisions of the present Agreement;

b) a commitment of the Contractor or sub-contractor to ensure that their premises have necessary conditions for handling and storing Classified Information of a given security classification level;

c) a commitment of the Contractor or sub-contractor to ensure that persons who perform duties requiring access to Classified Information are duly authorised in accordance to their national legislation to have access to Classified Information of the equivalent security classification level and have been regularly security briefed;

d) a list of Classified Information and list of areas in which Classified Information can be handled and stored;

e) a commitment to communicate any change in the security classification level of Classified Information.

f) the procedure for the transmission of Classified Information;

g) a commitment of the Contractor or sub-contractor to notify to their relevant National Security Authority of any actual or suspected Breach of Security;

h) a commitment of the Contractor or sub-contractor to forward a copy of the Classified Contract to the National Security Authority of both Parties.

3. A Facility Security Clearance and/or Personnel Security Clearance is not required for Classified Contracts that are limited to Classified Information marked as RISERVATO / ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ /RESTRICTED. These Classified Contracts shall contain an appropriate security requirement clause defining the minimum security requirement to be applied by the Contractor to Classified Information that is generated and/or provided as a result of the Contract. The security clause shall include a provision concerning the appointment, by the Contractor, of a person who has the overall responsibility of the protection of Classified Information marked as RISERVATO / ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ /RESTRICTED. A copy of the security requirement provision shall be provided to the National Security Authority, only upon request.

4. For industrial security purposes only, under the Italian legislation the points of entry and exit of Classified Information, within the meaning of paragraph 6 Article 6 of the present Agreement, are the security bodies of the Contractors or sub-contractors holding a Facility Security Clearance.

Article 10
Classified Visits

1. Governmental official visits involving access to Classified Information marked as SEGRETISSIMO / ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ /TOP SECRET, SEGRETO / ΑΠΟΡΡΗΤΟ /SECRET, and RISERVATISSIMO / ΕΜΠΙΣΤΕΥΤΙΚΟ / CONFIDENTIAL level shall be carried out upon submission of a Personnel Security Clearance prior to the visit.

2. All other types of visits, not provided by paragraph 1, for the purposes of this Agreement, involving access to Classified Information marked as ΕΜΠΙΣΤΕΥΤΙΚΟ/RISERVATISSIMO/CONFIDENTIAL and SEGRETO / ΑΠΟΡΡΗΤΟ /SECRET level, shall be subject to prior written approval given by the National Security Authority of the host Party.

3. The National Security Authority of the host Party shall receive a request for a visit at least 20 (twenty) days in advance.

4. In urgent cases, the request for a visit can be transmitted in shorter time.

5. The request for a visit shall include:

a) the visitor's name and surname, place and date of birth, citizenship, passport or identification document number;

b) the name of the legal person represented by the visitor and position of the visitor in the legal entity;

c) the name, address and contact information of the legal entity and the facility to be visited;

d) the confirmation of the visitor's Personnel Security Clearance, its validity and level;

e) the object and purpose of the visit and the highest Security Classification Level of Classified Information to be involved;

f) the expected date and duration of the requested visit. In case of recurring visits the total period covered by the visits shall be stated;

g) the date, signature and the official seal of the relevant authorised security body.

6. Once the visit has been approved, the National Security Authority of the host Party shall provide a copy of the request for visit to the security officers of the legal entity to be visited.

7. The validity of visit approval shall not exceed one year.

8. The National Security Authorities of the Parties may draw up lists of individuals authorised to make recurring visits. These lists shall be valid for an initial period of twelve months. The terms of the respective visits shall be directly arranged with the appropriate points of contact in the legal entity to be visited by these individuals, in accordance with the terms and conditions agreed upon.

Article 11
Breach of Security

1. In case of Breach of Security, the National Security Authority of the Receiving Party shall inform the National Security Authority of the Providing Party, as soon as possible, and initiate the appropriate investigation.

2. If a Breach of Security occurs in a third country, the National Security Authority of the Party who released the information to the third country shall take all necessary measures in order to ensure that the actions prescribed in Paragraph 1 are initiated.

3. The Providing Party shall, upon request, cooperate in the investigation in accordance to paragraph 1.

4. The Providing Party shall be informed of the results of the investigation and shall receive the final report on the causes and degree of damage.

Article 12
Expenses

1. For the implementation of this Agreement no expenses are needed.

2. Without prejudice to paragraph 1, each Party shall bear its possible unexpected expenses incurred in the course of application and supervision of this Agreement.

Article 13
Settlement of Disputes

Any dispute regarding the interpretation or application of this Agreement shall be settled by negotiations between the Parties.

Article 14
Final Provisions

1. This Agreement is valid for an indefinite period of time and enters into force on the first day of the second month after the date of the receipt of the last written notification by which the Parties have notified each other, through diplomatic channels, that their national legal requirements necessary for its entry into force have been fulfilled.

2. This Agreement may be amended any time on the basis of mutual written approval of the Parties. The amendments shall enter into force in accordance with paragraph 1.

3. Each Party may, at any time, terminate this Agreement by written notification to the other Party, through diplomatic channels. In this case, the termination takes effect six months after the date of the receipt of the respective notification.

4. Notwithstanding the termination of this Agreement, the Parties shall ensure that all Classified Information shall continue to be protected until the Providing Party exonerates the Receiving Party from this obligation.

Done at Nicosia on 31 July 2017 in two original sets, each in the Italian, Greek and English languages, all texts being equally authentic. In case of any divergence of interpretation, the English text shall prevail.

For the Government of the Italian Republic

For the Government of the Republic of Cyprus