

**ACCORDO**

**TRA**

**IL GOVERNO DELLA REPUBBLICA ITALIANA**

**E**

**IL GOVERNO DEL REGNO UNITO  
DI GRAN BRETAGNA E IRLANDA DEL NORD**

**PER LA**

**PROTEZIONE DELLE INFORMAZIONI CLASSIFICATE**

(denominate "Le Parti")

desiderando assicurare la protezione delle Informazioni Classificate generate o fornite dalle Parti, hanno concluso questo accordo, che disciplina le procedure e le misure di sicurezza relative a tale protezione, nell'interesse della sicurezza nazionale, ivi incluse la cooperazione politica, militare, economica, legale, scientifica e tecnologica o di ogni altro tipo.

## ARTICOLO 1 SCOPO

Lo scopo di questo Accordo è quello di assicurare la protezione delle Informazioni Classificate fornite da una Parte all'altra o generate congiuntamente da entrambe le Parti, e di agevolare il trasferimento in sicurezza e la conservazione di tali Informazioni Classificate scambiate tra le Parti, tra una Parte ed un suo Contraente o tra Contraenti, in conformità con le loro leggi ed i loro regolamenti nazionali.

## ARTICOLO 2 DEFINIZIONI

Ai fini di questo Accordo, i seguenti termini significano:

- a) **Informazione Classificata:** ogni informazione o attività, indipendentemente dalla sua forma, generata o scambiata tra le Parti o tra Contraenti soggetti alla loro giurisdizione, a cui è stato attribuito un Livello di Classifica di Segretezza in conformità con le leggi ed i regolamenti nazionali di una o di entrambe le Parti.
- b) **Contratto Classificato:** un contratto (o subcontratto o negoziazioni pre-contrattuali) che contenga Informazioni Classificate o che comporti l'accesso, la creazione, l'uso o la trasmissione di Informazioni Classificate.
- c) **Autorità Competente per la Sicurezza (ACS):** un'autorità governativa di una Parte responsabile dell'attuazione di questo Accordo.
- d) **Contraente:** una persona fisica o giuridica, diversa dalle Parti di questo Accordo, che abbia la capacità giuridica di assumere gli obblighi derivanti da un contratto.
- e) **Infrastruttura:** un'installazione, impianto, fabbrica, laboratorio, ufficio, università o altra istituzione educativa o impresa commerciale (inclusi eventuali annessi magazzini, aree di stoccaggio, servizi e componenti che, ove correlati per funzione e ubicazione, formino un'entità operativa) nonché qualsiasi dipartimento governativo, agenzia o impresa.
- f) **Abilitazione di Sicurezza Industriale:** una decisione assunta dall'Autorità Nazionale di Sicurezza o da un'Autorità Competente per la Sicurezza che attesta che un Contraente è dotato di appropriate misure di sicurezza all'interno di una specifica Infrastruttura, al fine di svolgere attività connesse ad un Contratto Classificato, in maniera tale da salvaguardare le Informazioni Classificate fino ad un determinato Livello di Classifica di Segretezza.

- g) **Autorità Nazionale di Sicurezza (ANS):** l'autorità governativa di una Parte, che detiene la responsabilità generale concernente la sicurezza delle Informazioni Classificate.
- h) **Necessità di Conoscere:** il principio in base al quale l'accesso ad Informazioni Classificate può essere consentito ad un individuo solo se necessario per lo svolgimento delle sue funzioni istituzionali.
- i) **Parte Fornitrice:** la Parte che fornisce Informazioni Classificate alla Parte Ricevente.
- j) **Abilitazione di Sicurezza Personale:** una decisione assunta dall'Autorità Nazionale di Sicurezza (ANS) o dall'Autorità Competente per la Sicurezza (ACS) al termine di una procedura investigativa svolta in conformità con le proprie leggi ed i propri regolamenti nazionali, che autorizza un individuo ad accedere ed a trattare Informazioni Classificate fino ad un determinato Livello di Classifica di Segretezza.
- k) **Parte Ricevente:** la Parte che riceve Informazioni Classificate dalla Parte Fornitrice.
- l) **Livello di Classifica di Segretezza:** la categoria assegnata ad una Informazione Classificata che ne indica la sensibilità, il livello di protezione che le Parti devono garantire ad essa, ed il grado di danno che potrebbe derivare nel caso di accesso non autorizzato, divulgazione, perdita o compromissione della stessa.
- m) **Incidente di Sicurezza:** Un atto od omissione che risulti o potrebbe risultare nell'accesso non autorizzato ad Informazioni Classificate, ovvero alla divulgazione, perdita o compromissione delle stesse.
- n) **Parte Terza:** Ogni Stato, organizzazione e persona giuridica che non è parte del presente Accordo ne' parte di un Contratto Classificato.
- o) **Visita:** Una visita autorizzata da parte di funzionari del Governo, o rappresentanti di un Contraente sotto la responsabilità dell'altra Parte, che comporti l'accesso e la trattazione di Informazioni Classificate.

### **ARTICOLO 3 AUTORITA' DI SICUREZZA**

(1) Le ANS designate dalle Parti sono:

Per la Repubblica Italiana:

- Presidenza del Consiglio dei Ministri  
Dipartimento delle Informazioni per la Sicurezza  
Ufficio Centrale per la Segretezza (DIS/UCSe)

Per il Regno Unito di Gran Bretagna ed Irlanda del Nord:

- UK National Security Authority, Cabinet Office

(2) Le ANS si informano reciprocamente rispetto ad ogni ACS responsabile per l'implementazione di questo Accordo e di ogni cambiamento rilevante a tali ACS.

(3) Allo scopo di raggiungere e mantenere livelli di sicurezza comparabili, le ANS hanno l'obbligo di fornire, su richiesta, informazioni appropriate circa i propri livelli, procedure e pratiche nazionali di sicurezza per la salvaguardia di Informazioni Classificate, eventualmente facilitando, a tal fine, visite dei rappresentanti dell'altra Parte, ove appropriato.

**ARTICOLO 4**  
**LIVELLI DI CLASSIFICHE DI SEGRETEZZA**

(1) Le Informazioni Classificate fornite fisicamente o elettronicamente ai sensi del presente Accordo devono essere contrassegnate con il Livello di Classifica di Segretezza appropriato, in conformità con le leggi ed i regolamenti della Parte Fornitrice.

(2) Le Parti stabiliscono la corrispondenza dei Livelli delle Classifiche di Segretezza nazionali come indicato nella seguente tabella di equivalenza:

| <b>Per la Repubblica Italiana</b> | <b>Per il Regno Unito di Gran Bretagna e Irlanda del Nord</b>                              |
|-----------------------------------|--------------------------------------------------------------------------------------------|
| SEGRETISSIMO                      | UK TOP SECRET                                                                              |
| SEGRETO                           | UK SECRET                                                                                  |
| RISERVATISSIMO                    | Nessun Livello di Classifica equivalente<br><i>(vedi paragrafo (3) di questo Articolo)</i> |
| RISERVATO                         | UK OFFICIAL-SENSITIVE                                                                      |

(3) Il Regno Unito ha l'obbligo di garantire alle Informazioni Classificate a livello RISERVATISSIMO lo stesso grado di protezione garantito alle Informazioni Classificate al livello UK SECRET.

**ARTICOLO 5**  
**PRINCIPI PER LA PROTEZIONE DELLE INFORMAZIONI CLASSIFICATE**

(1) Le Parti hanno l'obbligo di garantire alle Informazioni Classificate generate e/o fornite ai sensi del presente Accordo lo stesso grado di protezione garantito alle proprie Informazioni Classificate al Livello di Classifica di Segretezza corrispondente, in conformità con quanto disciplinato dall'Art. 4 paragrafo 2 di questo Accordo.

(2) La Parte Fornitrice deve:

- a) assicurare che ogni Informazione Classificata fornita alla Parte Ricevente sia contrassegnata con il Livello di Classifica di Segretezza appropriato. Ove l'Informazione Classificata sia fornita oralmente, la Parte Ricevente deve essere informata del Livello di Classifica di Segretezza ad essa attribuito;
- b) informare, ove appropriato, la Parte Ricevente od il Contraente di qualsiasi condizione di rilascio o limitazione d'uso delle Informazioni Classificate fornite;
- c) informare la Parte Ricevente od il Contraente di qualsiasi successiva modifica al Livello di Classifica di Segretezza di ogni Informazione Classificata fornita.

(3) Quando una Parte fornisce Informazioni Classificate ad una Parte Ricevente, la Parte Ricevente deve:

- a) assicurare che il Livello di Classifica di Segretezza assegnato all'Informazione Classificata non sia modificato o revocato, eccetto in caso di previo consenso scritto della Parte Fornitrice;

- b) assicurare che tali Informazioni Classificate siano utilizzate solo per i fini per i quali sono state fornite e nel rispetto di ogni limitazione stabilita dalla Parte Fornitrice;
- c) subordinatamente all'Articolo 7 di questo Accordo ed alle leggi ed i regolamenti nazionali applicabili, non divulgare tali Informazioni Classificate a Parti Terze, ovvero renderle disponibili al pubblico senza il previo consenso scritto della Parte Fornitrice.

(4) Ciascuna Parte ha l'obbligo di notificare all'altra Parte qualsiasi modifica significativa alla propria legislazione o ai propri regolamenti nazionali, che incidano sostanzialmente sulla protezione delle Informazioni Classificate generate e/o fornite ai sensi del presente Accordo.

## **ARTICOLO 6**

### **ACCESSO ALLE INFORMAZIONI CLASSIFICATE E ABILITAZIONI DI SICUREZZA PERSONALI**

(1) L'accesso ad Informazioni Classificate a livello SEGRETISSIMO, UK TOP SECRET, SEGRETO, UK SECRET o RISERVATISSIMO è consentito solo a soggetti che siano in possesso di Abilitazione di Sicurezza Personale al livello adeguato, che abbiano Necessità di Conoscere e che siano stati istruiti circa le proprie responsabilità in materia di protezione delle Informazioni Classificate. In via eccezionale, a determinati soggetti può essere consentito di accedere ad Informazioni Classificate in ragione delle loro funzioni, se permesso dalle rispettive leggi e dai rispettivi regolamenti nazionali.

(2) Ai fini di questo Accordo, le Parti hanno l'obbligo di riconoscimento reciproco delle Abilitazioni di Sicurezza Personali rilasciate dall'altra Parte.

(3) Le Parti, su richiesta ed in conformità con le proprie leggi e regolamenti nazionali applicabili, hanno l'obbligo di prestarsi reciproca assistenza nello svolgimento dei controlli su soggetti che risiedano o abbiano risieduto nei loro Paesi necessari per il rilascio dell'Abilitazione di Sicurezza Personale.

(4) L'accesso ad Informazioni Classificate a livello SEGRETISSIMO o UK TOP SECRET da parte di un soggetto munito di Abilitazione di Sicurezza Personale corrispondente almeno a quel livello di Classifica e in possesso della sola cittadinanza italiana o britannica, ovvero la doppia cittadinanza italiana e britannica, può essere consentito senza il previo consenso scritto della Parte Fornitrice.

(5) L'accesso ad Informazioni Classificate a livello SEGRETISSIMO o UK TOP SECRET da parte di un soggetto munito di Abilitazione di Sicurezza Personale corrispondente almeno a quel livello di Classifica che non abbia le caratteristiche di nazionalità indicate nel paragrafo (4) di questo articolo necessita del previo consenso scritto della Parte Fornitrice.

(6) L'accesso ad Informazioni Classificate a livello SEGRETO, UK SECRET o RISERVATISSIMO da parte di un soggetto munito di Abilitazione di Sicurezza Personale corrispondente almeno a quei livelli di Classifica e in possesso di cittadinanza italiana, britannica, o doppia cittadinanza di cui almeno una risulti essere italiana o britannica, può essere consentito senza il previo consenso scritto della Parte Fornitrice.

(7) L'accesso ad Informazioni Classificate a livello SEGRETO, UK SECRET o RISERVATISSIMO da parte di un soggetto munito di Abilitazione di Sicurezza Personale corrispondente almeno a quei livelli di Classifica che non abbia le caratteristiche di nazionalità indicate nel paragrafo (6) di questo articolo necessita del previo consenso scritto della Parte Fornitrice.

(8) Se, in conformità con le leggi ed i regolamenti nazionali applicabili, una ANS o ACS rimuove o abbassa il livello di un'Abilitazione di Sicurezza Personale precedentemente rilasciata ed in relazione

alla quale sia stata fornita conferma all'altra Parte, essa ha l'obbligo di notificarlo all'ANS o all'ACS responsabile dell'altra Parte per iscritto, non appena possibile, ove appropriato.

(9) Niente in questo Accordo deve influire sulla facoltà delle Parti di consentire l'accesso ad Informazioni Classificate in conformità con l'Art. 23 del Framework Agreement concerning Measures to Facilitate the Restructuring and Operation of the European Defence Industry, firmato a Farnborough il 27 luglio 2000 (di seguito "EDIR Framework Agreement").

10) L'Abilitazione di Sicurezza Personale non è necessaria per accedere ad Informazioni Classificate a livello RISERVATO o UK OFFICIAL-SENSITIVE. Tale accesso deve essere limitato a soggetti che abbiano necessità di conoscere e che siano stati debitamente istruiti circa le proprie responsabilità ed obblighi connessi alla protezione di tali Informazioni Classificate.

## **ARTICOLO 7 DIVULGAZIONE DI INFORMAZIONI CLASSIFICATE**

(1) Nell'ambito delle proprie leggi e dei propri regolamenti nazionali, la Parte Ricevente deve adottare tutte le misure ragionevolmente disponibili per evitare che Informazioni Classificate fornite ai sensi del presente Accordo siano rese disponibili al pubblico.

(2) In caso di richiesta di rendere disponibile al pubblico qualsiasi Informazione Classificata fornita ai sensi di questo Accordo, la Parte Ricevente ha l'obbligo di notificare immediatamente tale richiesta per iscritto alla Parte Fornitrice, ed entrambe le Parti hanno l'obbligo di reciproca consultazione per iscritto prima che una decisione di divulgazione sia presa dalla Parte Ricevente.

## **ARTICOLO 8 TRASMISSIONE DI INFORMAZIONI CLASSIFICATE**

(1) Nel caso in cui una Parte desideri trasmettere Informazioni Classificate a livello SEGRETISSIMO o UK TOP SECRET in forma fisica, essa deve adottare le misure necessarie affinché l'Informazione Classificata sia trasportata nel territorio dell'altra Parte attraverso canali governativi.

(2) Nel caso in cui una Parte desideri trasmettere Informazioni Classificate a livello SEGRETO, UK SECRET o RISERVATISSIMO in forma fisica, essa deve adottare le misure necessarie affinché l'Informazione Classificata sia trasportata nel territorio dell'altra Parte attraverso canali governativi o attraverso altri canali sicuri reciprocamente approvati dalle ANS o dalle ACS responsabili di entrambe le Parti.

(3) In casi di urgenza, Informazioni Classificate a livello RISERVATISSIMO possono essere trasmesse tramite corrieri commerciali autorizzati dall'ANS italiana.

4) Nel caso in cui una Parte trasmetta Informazioni Classificate a livello SEGRETISSIMO, UK TOP SECRET, SEGRETO, UK SECRET o RISERVATISSIMO in forma fisica, essa ha l'obbligo di accludere ricevuta di firma da parte o per conto della Parte Ricevente o del Contraente ricevente, che deve essere riconsegnata entro la data specificata nella ricevuta.

(5) Nel caso in cui una Parte desideri trasmettere Informazioni Classificate a livello RISERVATO o UK OFFICIAL-SENSITIVE in forma fisica, queste possono essere trasportate nel territorio dell'altra Parte tramite servizio postale internazionale, corriere commerciale, a mano ad opera di personale autorizzato o tramite canali diplomatici.

(6) In caso di trasmissione in forma fisica di spedizioni voluminose contenenti Informazioni Classificate, le procedure di trasporto devono essere esaminate e approvate congiuntamente dalle ANS o dalle ACS responsabili di entrambe le Parti.

(7) In caso di trasmissione in forma fisica di Informazioni Classificate a livello SEGRETISSIMO, UK TOP SECRET, SEGRETO, UK SECRET o RISERVATISSIMO dal territorio di una Parte al territorio dell'altra Parte via cargo, il trasporto deve essere esaminato e approvato congiuntamente dalle ANS o dalle ACS responsabili di entrambe le Parti. L'ANS o la responsabile ACS del mittente deve fornire all'ANS o alla responsabile ACS dell'Infrastruttura ricevente, prima dell'inizio del trasporto, un piano di trasporto per approvazione. Il piano di trasporto deve contenere, almeno, le seguenti informazioni:

- a) i nomi ed i numeri di carta d'identità/passaporto del personale coinvolto nel trasporto;
- b) il livello e la validità dell'Abilitazione di Sicurezza Personale per tutto il personale direttamente coinvolto nel trasporto;
- c) ove appropriato, conferma dell'Abilitazione di Sicurezza Industriale della compagnia di trasporto;
- d) una lista delle Informazioni Classificate che saranno trasportate via cargo, compreso il Livello di Classifica di Segretezza di tali informazioni;
- e) i dettagli del programma di trasporto, compresi l'orario di partenza, orario di consegna atteso ed eventuali fermate e pernottamenti;
- f) i dettagli del percorso pianificato, comprensivi dei mezzi di trasporto utilizzati.

Deviazioni dal piano di trasporto originario non sono permesse a meno che non siano necessarie per esigenze connesse ad incidenti imprevisti.

(8) Nel caso in cui una Parte desideri trasmettere Informazioni Classificate in forma elettronica, essa ha l'obbligo di trasmetterle in forma crittografata, utilizzando metodi e strumenti di crittografia accettati da entrambe le Parti.

(9) A titolo di eccezione al paragrafo (8) di questo articolo, nel caso in cui una Parte desideri trasmettere Informazioni Classificate a livello UK OFFICIAL-SENSITIVE in forma elettronica, tale trasmissione può essere effettuata in chiaro laddove metodi e strumenti crittografici idonei non siano disponibili, e se permesso dall'ACS responsabile del Regno Unito. Ove ciò non sia permesso, le Informazioni Classificate devono essere protette attraverso metodi e strumenti di crittografia accettati da entrambe le Parti. Questo paragrafo non si applica ad Informazioni Classificate a livello SEGRETISSIMO, UK TOP SECRET, SEGRETO, UK SECRET, RISERVATISSIMO e RISERVATO.

## **ARTICOLO 9 RIPRODUZIONE, TRADUZIONE E DISTRUZIONE DI INFORMAZIONI CLASSIFICATE**

(1) Riproduzioni e traduzioni devono mantenere il Livello di Classifica di Segretezza applicato all'originale e devono essere protette in conformità con le disposizioni del presente Accordo. Tali riproduzioni e traduzioni devono essere limitate al minimo indispensabile ed effettuate soltanto da individui in possesso di Abilitazione di Sicurezza Personale al livello appropriato.

(2) Le Traduzioni devono recare appropriato contrassegno, nella lingua di traduzione, indicante che esse contengono Informazioni Classificate della Parte Fornitrice.

(3) Informazioni Classificate a livello SEGRETISSIMO o UK TOP SECRET possono essere riprodotte o tradotte solo previa autorizzazione scritta della Parte Fornitrice.

(4) A meno di previo consenso scritto rilasciato dalla Parte Fornitrice, le Informazioni Classificate a livello **SEGRETISSIMO** o **UK TOP SECRET** non più necessarie non devono essere distrutte dalla Parte Ricevente, bensì riconsegnate alla Parte Fornitrice in conformità con l'Art. 8 del presente Accordo.

(5) Ove non più necessarie, Informazioni Classificate recanti contrassegno **SEGRETO**, **UK SECRET** o **RISERVATISSIMO** devono essere distrutte conformemente ai parametri ed i metodi che la Parte Ricevente è tenuta ad applicare alle proprie Informazioni Classificate al Livello di Classifica di Segretezza equivalente. La Parte Ricevente deve informare la Parte Fornitrice di tale distruzione.

(6) Ove non più necessarie, Informazioni Classificate recanti contrassegno **RISERVATO** o **UK OFFICIAL-SENSITIVE** devono essere distrutte conformemente ai parametri ed i metodi che la Parte Ricevente è tenuta ad applicare alle proprie Informazioni Classificate al Livello di Classifica di Segretezza equivalente.

(7) In situazioni di crisi che rendano impossibile per la Parte Ricevente proteggere o restituire Informazioni Classificate generate e/o fornite dalla Parte Fornitrice, le Informazioni Classificate devono essere distrutte non appena possibile utilizzando ogni strumento appropriato al fine di evitare Incidenti di Sicurezza. L'ANS o la responsabile ACS della Parte Ricevente deve informare l'ANS o la responsabile ACS della Parte Fornitrice per iscritto nel caso in cui Informazioni Classificate fornite ai sensi del presente Accordo siano state distrutte in tali situazioni.

(8) La Parte Fornitrice può vietare la riproduzione, traduzione o distruzione delle sue Informazioni Classificate apponendo appropriato contrassegno, allegando notifica scritta, o fornendo alla Parte Ricevente istruzioni per la trattazione.

## **ARTICOLO 10 CONTRATTI CLASSIFICATI E ABILITAZIONI DI SICUREZZA INDUSTRIALI**

(1) Nel caso in cui una Parte proponga la conclusione di un Contratto Classificato che comporti la trattazione di Informazioni Classificate a livello **SEGRETISSIMO**, **UK TOP SECRET**, **SEGRETO**, **UK SECRET** o **RISERVATISSIMO** con un Contraente sottoposto alla giurisdizione dell'altra Parte, l'ANS o ACS responsabile della Parte proponente il contratto ha l'obbligo di ottenere previa conferma scritta dall'ANS o ACS responsabile dell'altra Parte che il Contraente sottoposto alla giurisdizione di essa è in possesso di Abilitazione di Sicurezza Personale e/o Abilitazione di Sicurezza Industriale almeno al Livello di Classifica di Segretezza appropriato.

(2) L'ANS o ACS che ha rilasciato l'Abilitazione di Sicurezza Personale o Abilitazione di Sicurezza Industriale è responsabile, in conformità con le proprie leggi e regolamenti nazionali, del monitoraggio delle condotte di sicurezza del Contraente o dell'individuo abilitato.

(3) Ai fini di questo Accordo, la Parte Fornitrice ha l'obbligo di riconoscere le Abilitazioni di Sicurezza Industriali rilasciate dall'ANS o dalla ACS della Parte Ricevente.

(4) Una Parte che, dopo l'entrata in vigore del presente Accordo, entri o proponga di entrare in un Contratto Classificato che comporti la trattazione di Informazioni Classificate a livello **SEGRETISSIMO**, **UK TOP SECRET**, **SEGRETO**, **UK SECRET** o **RISERVATISSIMO**, ha l'obbligo di assicurare che il Contraente sia giuridicamente obbligato a garantire all'Informazione Classificata ricevuta dall'altra Parte lo stesso livello di protezione accordato dalla Parte Ricevente ai sensi di questo Accordo.

(5) Una Parte ha l'obbligo di assicurare che tutti i Contratti Classificati contengano disposizioni che riflettano sostanzialmente i requisiti di sicurezza rilevanti per la tutela delle Informazioni

Classificate vincolanti per le Parti per effetto di questo Accordo. Per i Contratti Classificati a livello SEGRETISSIMO, UK TOP SECRET, SEGRETO, UK SECRET o RISERVATISSIMO, una copia del Contratto Classificato deve essere trasmessa all'ANS o ACS responsabile della Parte Ricevente al fine di facilitare il monitoraggio degli aspetti di sicurezza di esso.

(6) Nei casi in cui l'ANS o ACS responsabile della Parte Ricevente rimuova o abbassi il livello dell'Abilitazione di Sicurezza Industriale rilasciata all' Infrastruttura di un Contraente che tratti o conservi Informazioni Classificate generate e/o fornite ai sensi del presente Accordo, l'ANS o ACS responsabile della Parte Fornitrice deve essere informata non appena possibile.

(7) Ove la Parte Fornitrice abbia valide ragioni relative ad aspetti di sicurezza per sospettare che l' Infrastruttura di un Contraente in possesso di Abilitazione di Sicurezza Industriale, situata nel territorio dell'altra Parte non stia adeguatamente proteggendo le sue Informazioni Classificate, l'ANS della Parte Fornitrice può richiedere che un'ispezione di sicurezza sia condotta dall'ANS o dall'ACS responsabile della Parte Ricevente allo scopo di verificare l'ottemperanza di dette Infrastrutture alle norme a tutela delle Informazioni Classificate.

(8) L'Abilitazione di Sicurezza Industriale non è necessaria in relazione a Contratti Classificati che comportino la trattazione di Informazioni Classificate al livello RISERVATO o UK OFFICIAL-SENSITIVE. Una Parte che concluda o proponga di concludere, dopo l'entrata in vigore di questo Accordo, un Contratto Classificato che comporti la trattazione di Informazioni Classificate al livello RISERVATO o UK OFFICIAL-SENSITIVE ha l'obbligo di garantire che esso contenga un'adeguata clausola sui requisiti di sicurezza, che definisce i requisiti di sicurezza minimi che il Contraente deve applicare alle Informazioni Classificate generate e/o fornite in applicazione di tale Contratto. La clausola sui requisiti di sicurezza dovrebbe contenere una disposizione relativa alla nomina, da parte del Contraente, di una persona cui è attribuita la responsabilità generale per la protezione di Informazioni Classificate con il contrassegno RISERVATO o UK OFFICIAL-SENSITIVE.

## **ARTICOLO 11 VISITE**

(1) Se un funzionario di una Parte ha necessità di visitare un dipartimento governativo, un'agenzia o una struttura posta sotto la responsabilità dell'altra Parte, e tale visita comporta o potrebbe comportare l'accesso a Informazioni Classificate a livello SEGRETISSIMO, UK TOP SECRET, SEGRETO, UK SECRET o RISERVATISSIMO, il visitatore deve assicurare che i dettagli della sua Abilitazione di Sicurezza Personale siano forniti alla struttura ospitante prima della visita.

(2) Se un funzionario di una Parte ha necessità di visitare un'Infrastruttura di un Contraente a cui è stata rilasciata un'Abilitazione di Sicurezza Industriale dall'altra Parte, e questa visita comporta o potrebbe comportare l'accesso ad Informazioni Classificate a livello SEGRETISSIMO, UK TOP SECRET, SEGRETO, UK SECRET o RISERVATISSIMO, si applica la procedura disciplinata dai paragrafi (3), (4) e (5) di questo Articolo.

(3) Una richiesta di visita ai sensi del paragrafo (2) di questo Articolo deve essere trasmessa dall'ANS o dall'ACS responsabile del visitatore all'ANS o all'ACS responsabile della Infrastruttura ospitante almeno 20 giorni lavorativi prima dell'inizio della visita. La richiesta di visita deve comprendere almeno le seguenti informazioni:

- a) il nome, data e luogo di nascita, nazionalità e numero di carta d'identità/passaporto del visitatore;
- b) qualifica ufficiale del visitatore ed il nome dell'organizzazione che questi rappresenta;
- c) data e durata della visita. In caso di visite ricorrenti, deve essere indicato il periodo complessivo coperto dalle visite;
- d) lo scopo della visita e le materie oggetto di discussione;

- e) il nome, indirizzo, numero di telefono, indirizzo email e punto di contatto dell'Infrastruttura oggetto di visita;
- f) l'indicazione del più alto Livello di Classifica di Segretezza delle Informazioni che saranno oggetto di discussione o accesso;
- g) il livello e la validità dell'Abilitazione di Sicurezza Personale del visitatore; e
- h) data e firma di un rappresentante dell'ANS o dell'ACS responsabile del visitatore (o persona che agisca per suo conto), debitamente autorizzato a formulare tale richiesta di visita.

(4) In casi urgenti, le ANS o ACS responsabili di entrambe le Parti possono concordare termini più brevi rispetto a quelli indicati nel paragrafo (3) di questo articolo per le richieste di visita.

(5) Per specifici Contratti Classificati o programmi è possibile, subordinatamente al consenso delle ANS o delle ACS responsabili di entrambe le Parti, istituire una lista dei visitatori ricorrenti. Tale lista è valida per un periodo iniziale che non eccede 12 mesi dalla data di autorizzazione e può essere esteso per ulteriori periodi di tempo non eccedenti 12 mesi, subordinatamente al reciproco accordo delle ANS o ACS responsabili. La lista dei visitatori periodici deve essere trasmessa, conformemente ai paragrafi (3) e (4) di questo Articolo. A seguito dell'autorizzazione di tale lista, le visite possono essere organizzate direttamente tra i visitatori e l'Infrastruttura ospitante, senza ulteriore coinvolgimento delle ANS o ACS responsabili.

(6) Le visite hanno luogo soltanto quando le richieste di visita descritte nei paragrafi (3), (4) e (5) di questo Articolo sono state autorizzate dall'ANS o dall'ACS responsabile della Infrastruttura ospitante.

(7) Le ANS o ACS di entrambe le Parti possono decidere che procedure di visita alternative a quelle descritte nei paragrafi (3), (4), (5) e (6) di questo Articolo possano essere adottate per specifici Contratti Classificati o programmi. Tali procedure di visita alternative devono essere reciprocamente concordate e possono essere inserite all'interno delle Istruzioni di Sicurezza del Programma.

(8) Nulla in questo Accordo ha impatto sulle visite disciplinate dall'EDIR Framework Agreement.

(9) Le visite che comportano accesso ad Informazioni Classificate a livello RISERVATO o UK OFFICIAL-SENSITIVE sono organizzate direttamente tra il visitatore e l'Infrastruttura ospitante oggetto di visita.

## **ARTICOLO 12 INCIDENTI DI SICUREZZA**

(1) Subordinatamente al paragrafo (2) del presente articolo, qualsiasi Incidente di Sicurezza reale o presunto che ha luogo nel territorio di una Parte o presso una Infrastruttura per la quale una Parte è responsabile (compresa la missione diplomatica di tale Parte), deve essere immediatamente oggetto di indagine ad opera di quella Parte.

2) Nel caso in cui un Incidente di Sicurezza sia confermato dalla Parte inquirente, tale Parte deve adottare, in conformità con le sue leggi ed i suoi regolamenti nazionali applicabili, le misure atte a limitare le conseguenze dell'incidente e prevenirne il ripetersi.

(3) Nel caso in cui un Incidente di Sicurezza comporti la compromissione di Informazioni Classificate, l'ANS della Parte sul cui territorio si è verificato l'incidente, o l'ANS della Parte responsabile dell'Infrastruttura coinvolta, deve informare il prima possibile e per iscritto l'altra ANS dell'esito dell'indagine e delle misure adottate per prevenire il ripetersi dell'Incidente.

(4) Nel caso in cui un Incidente di Sicurezza che coinvolge Informazioni Classificate si verifichi al di fuori dei territori dell'Italia o del Regno Unito, l'ANS o ACS responsabile deve adottare le misure appropriate per limitare le conseguenze dell'Incidente di Sicurezza e informare l'altra ANS o ACS responsabile appena possibile.

### **ARTICOLO 13 DISPOSIZIONI FINANZIARIE**

Ciascuna Parte ha l'obbligo di sostenere i propri costi relativi all'implementazione di questo Accordo senza eccedere le proprie ordinarie dotazioni di bilancio.

### **ARTICOLO 14 SOLUZIONE DI CONTROVERSIE**

Qualsiasi controversia o disaccordo tra le parti relativi all'interpretazione o applicazione di questo Accordo deve essere risolta attraverso la consultazione tra le Parti stesse, e non potrà essere trasmessa ad una Terza Parte ai fini della soluzione.

### **ARTICOLO 15 DISPOSIZIONI FINALI**

(1) Ciascuna Parte ha l'obbligo di notificare all'altra Parte, attraverso note diplomatiche, il completamento delle procedure giuridiche interne necessarie per l'entrata in vigore di questo Accordo. Questo Accordo entra in vigore il primo giorno del secondo mese successivo al ricevimento dell'ultima notifica.

(2) Il presente Accordo si applica provvisoriamente dalla data di firma.

(3) Il presente Accordo può essere emendato in qualsiasi momento su richiesta di una delle due Parti. Gli emendamenti concordati entrano in vigore il primo giorno del secondo mese successivo allo scambio delle note diplomatiche.

(4) Le ANS o ACS possono concludere intese attuative ai sensi del presente Accordo.

(5) Il presente Accordo rimane in vigore fino a diversa notifica. Ciascuna Parte può terminare il presente Accordo inviando nota diplomatica all'altra Parte. In tal caso, l'Accordo cessa di avere efficacia trascorsi sei mesi dalla ricezione della notifica ad opera dell'altra Parte.

(6) In caso di cessazione di efficacia del presente Accordo, tutte le Informazioni Classificate generate e/o fornite dalle Parti devono continuare ad essere protette in conformità con le disposizioni in esso contenute. Su richiesta, tali Informazioni Classificate devono essere restituite in sicurezza dalla Parte Ricevente alla Parte Fornitrice.

(7) Dopo l'entrata in vigore del presente Accordo, la Parte nel cui territorio l'Accordo è concluso deve predisporre misure immediate per la registrazione dello stesso presso il Segretariato delle Nazioni Unite, conformemente all'Art. 102 della Carta ONU. La stessa Parte deve notificare all'altra parte

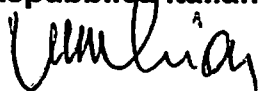
l'avvenuta registrazione ed il relativo numero nella Serie dei Trattati ONU, non appena emesso dal Segretariato ONU.

(8) All'entrata in vigore di questo Accordo, l'Accordo Generale di Sicurezza tra la Repubblica Italiana ed il Regno Unito di Inghilterra e Irlanda del Nord per la protezione delle informazioni classificate scambiate per fini di ricerca, sviluppo, produzione e approvvigionamento tra i due Paesi, datato 16 febbraio 2004 e le successive modifiche, cessa di produrre effetti. Ogni Informazione Classificata precedentemente generata e/o fornita nel quadro di tale Accordo deve essere protetta in conformità con le disposizioni del presente Accordo.

In fede di che i sottoscritti, debitamente autorizzati, hanno firmato questo Accordo.

Fatto a Roma il 22 settembre 2020 in due copie originali, in lingua Italiana ed Inglese, essendo entrambi i testi ugualmente autentici.

**Per il Governo della  
Repubblica Italiana:**



**Per il Governo del Regno Unito di Gran  
Bretagna e Irlanda del Nord:**



**AGREEMENT**

**BETWEEN**

**THE GOVERNMENT OF THE ITALIAN REPUBLIC**

**AND**

**THE GOVERNMENT OF THE UNITED KINGDOM OF  
GREAT BRITAIN AND NORTHERN IRELAND**

**CONCERNING THE**

**PROTECTION OF CLASSIFIED INFORMATION**

The Government of the Italian Republic

and

the Government of the United Kingdom of Great Britain and Northern Ireland

(referred to as the "Parties")

wishing to ensure the protection of Classified Information generated and/or provided by the Parties have, in the interests of national security, including political, military, economic, legal, scientific and technological or any other cooperation, concluded this Agreement which sets out the security procedures and arrangements for such protection.

## **ARTICLE 1 PURPOSE**

The purpose of this Agreement is to ensure the protection of Classified Information which has been provided by one Party to the other or which has been jointly generated by both Parties, and to facilitate the secure transfer and storage of such Classified Information exchanged between the Parties, between a Party and a Contractor, or between Contractors, in accordance with their national laws and regulations.

## **ARTICLE 2 DEFINITIONS**

For the purposes of this Agreement the following terms mean:

- a) **Classified Information:** Any information or assets, regardless of form, transmitted between or generated by the Parties, or Contractors under their jurisdiction, to which a Security Classification Level has been assigned in accordance with the national laws and regulations of one or both of the Parties.
- b) **Classified Contract:** A contract (or sub-contract or pre-contractual negotiations) which contains Classified Information or which involves access to, or the generation, use or transmission of Classified Information.
- c) **Competent Security Authority (CSA):** A Government authority of a Party which is responsible for the implementation of this Agreement.
- d) **Contractor:** Any natural or legal person with the capability to enter into contracts other than a Party to this Agreement.
- e) **Facility:** An installation, plant, factory, laboratory, office, university or other educational institution or commercial undertaking (including any associated warehouses, storage areas, utilities and components which, when related by function and location, form an operating entity), and any government department, agency or establishment.
- f) **Facility Security Clearance (FSC):** A determination by a NSA or CSA that a Contractor has in place appropriate security measures within a specified Facility to carry out activities related to a

Classified Contract in a way which shall safeguard Classified Information up to and including a particular Security Classification Level.

- g) **National Security Authority (NSA):** The Government authority of a Party with ultimate responsibility for the security of Classified Information.
- h) **Need-to-Know:** The principle whereby access to Classified Information may be granted to an individual only when it is necessary for the performance of his or her official duties.
- i) **Providing Party:** The Party which first provides Classified Information to the Receiving Party.
- j) **Personnel Security Clearance (PSC):** A determination by a NSA or CSA, following a vetting procedure undertaken in accordance with its national laws and regulations, that an individual is authorised to have access to and to handle Classified Information up to and including a particular Security Classification Level.
- k) **Receiving Party:** The Party which receives Classified Information from the Providing Party.
- l) **Security Classification Level:** A category assigned to Classified Information which indicates its sensitivity, the level of protection to be applied to it by the Parties, and the degree of damage that might arise in the event of its unauthorised access, disclosure, loss or compromise.
- m) **Security Incident:** An act or omission which results or has the potential to result in the unauthorised access to, disclosure, loss or compromise of Classified Information.
- n) **Third Party:** Any State, organisation and legal entity which is neither a party to this agreement nor a party to a Classified Contract.
- o) **Visit:** An authorised visit by Government officials, or representatives of a Contractor under the responsibility of the other Party, which involves access to and handling of Classified Information.

### **ARTICLE 3 SECURITY AUTHORITIES**

- (1) The NSAs designated by the Parties are:

For the Italian Republic:

- Presidenza del Consiglio dei Ministri  
Dipartimento delle Informazioni per la Sicurezza  
Ufficio Centrale per la Segretezza (DIS/UCSe)

For the United Kingdom of Great Britain and Northern Ireland:

- UK National Security Authority, Cabinet Office

- (2) The NSAs shall inform each other of any CSAs responsible for the implementation of this Agreement and of any significant changes to those CSAs.
- (3) In order to achieve and maintain comparable standards of security, the NSAs shall, on request, provide each other with appropriate information about their national security standards, procedures and practices for safeguarding Classified Information, and may for this purpose facilitate visits by representatives of the other Party as appropriate.

**ARTICLE 4**  
**SECURITY CLASSIFICATION LEVELS**

- (1) Classified Information provided physically or electronically under this Agreement shall be marked with the appropriate Security Classification Level in accordance with the national laws and regulations of the Providing Party.
- (2) The Parties agree that national Security Classification Levels shall correspond to each other as follows:

| <b>For the Italian Republic</b> | <b>For the United Kingdom of Great Britain and Northern Ireland</b> |
|---------------------------------|---------------------------------------------------------------------|
| SEGRETISSIMO                    | UK TOP SECRET                                                       |
| SEGRETO                         | UK SECRET                                                           |
| RISERVATISSIMO                  | No equivalent<br>(see paragraph (3) of this Article)                |
| RISERVATO                       | UK OFFICIAL-SENSITIVE                                               |

- (3) The UK shall afford Classified Information marked RISERVATISSIMO the same degree of protection as it would Classified Information at the level of UK SECRET.

**ARTICLE 5**  
**PRINCIPLES FOR THE PROTECTION OF CLASSIFIED INFORMATION**

- (1) The Parties shall afford to Classified Information generated and/or provided under this Agreement the same degree of protection as they would their own Classified Information at the corresponding Security Classification Level as set out in Article 4, paragraph (2) of this Agreement.
- (2) The Providing Party shall:
- ensure that any Classified Information provided to the Receiving Party is marked with an appropriate Security Classification Level. If the Classified Information is provided orally then the Receiving Party shall be informed of the Security Classification Level;
  - if appropriate, inform the Receiving Party or Contractor of any conditions of release or limitations on the use of any Classified Information provided; and
  - inform the Receiving Party or Contractor of any subsequent changes in the Security Classification Level of any Classified Information provided.
- (3) When a Party provides Classified Information to a Receiving Party, the Receiving Party shall:
- ensure that the Security Classification Level assigned to the Classified Information is not altered or revoked, except with the prior written approval of the Providing Party;
  - ensure that such Classified Information is used only for the purpose for which it has been provided and within any limitations stated by the Providing Party;

- c) subject to Article 7 of this Agreement and the applicable national laws and regulations, not disclose such Classified Information to a Third Party or make such Classified Information available to the public without the prior written approval of the Providing Party.
- (4) Each Party shall notify the other about any significant changes to their national laws and regulations which substantially affect the protection of Classified Information generated and/or provided under this Agreement.

## **ARTICLE 6**

### **ACCESS TO CLASSIFIED INFORMATION AND PERSONNEL SECURITY CLEARANCES**

- (1) Access to Classified Information at the SEGRETISSIMO, UK TOP SECRET, SEGRETO, UK SECRET or RISERVATISSIMO level shall be limited to those individuals who hold an appropriate PSC, have a Need-to-Know and have been briefed on their responsibilities to protect Classified Information. As an exception, certain individuals may be permitted access to Classified Information by virtue of their function if permitted under their respective national laws and regulations.
- (2) For the purpose of this Agreement the Parties shall mutually recognise PSCs issued by the other Party.
- (3) The Parties shall, upon request, and in accordance with their applicable national laws and regulations, assist each other in carrying out checks required for the PSC process, on individuals who reside or have resided in their country.
- (4) Access to Classified Information at the SEGRETISSIMO or UK TOP SECRET level by an individual holding a PSC to at least that level and holding single Italian or British nationality, or dual Italian and British nationality, may be granted without the prior written approval of the Providing Party.
- (5) Access to Classified Information at the SEGRETISSIMO or UK TOP SECRET level by an individual holding a PSC to at least that level and not holding the nationalities as set out in paragraph (4) of this Article shall require the prior written approval of the Providing Party.
- (6) Access to Classified Information at the SEGRETO, UK SECRET or RISERVATISSIMO level by an individual holding a PSC to at least that level and holding single Italian or British nationality, or holding dual nationality where at least one part is Italian or British, may be granted without the prior written approval of the Providing Party.
- (7) Access to Classified Information at the SEGRETO, UK SECRET or RISERVATISSIMO level by an individual holding a PSC to at least that level and not holding the nationalities as set out in paragraph (6) of this Article shall require the prior written approval of the Providing Party.
- (8) If, in accordance with its applicable national laws and regulations, a NSA or CSA withdraws or downgrades a PSC issued for which a confirmation has been provided to the other Party, they shall notify the NSA or relevant CSA of that other Party, as appropriate, in writing as soon as is practicable.
- (9) Nothing in this Agreement affects the ability of the Parties to grant access to Classified Information in accordance with Article 23 of the Framework Agreement concerning Measures to Facilitate the Restructuring and Operation of the European Defence Industry, signed at Farnborough on 27 July 2000 (hereinafter the "EDIR Framework Agreement").
- (10) A PSC is not required for access to Classified Information marked RISERVATO or UK OFFICIAL-SENSITIVE. Such access shall be limited to individuals who have a Need-to Know and

who have been appropriately briefed on their responsibilities and obligations to protect such Classified Information.

## **ARTICLE 7 DISCLOSURE OF CLASSIFIED INFORMATION**

- (1) Within the scope of its national laws and regulations the Receiving Party shall take all reasonable steps available to prevent Classified Information provided under this Agreement being made available to the public.
- (2) If there is any request to make any Classified Information provided under this Agreement available to the public, the Receiving Party shall immediately notify the Providing Party in writing, and both Parties shall consult each other in writing before a disclosure decision is taken by the Receiving Party.

## **ARTICLE 8 TRANSMISSION OF CLASSIFIED INFORMATION**

- (1) If a Party wishes to transmit Classified Information at the **SEGRETISSIMO** or **UK TOP SECRET** level in physical form it shall make arrangements for the Classified Information to be transmitted to the territory of the other Party through Government-to-Government channels.
- (2) If a Party wishes to transmit Classified Information at the **SEGRETO**, **UK SECRET** or **RISERVATISSIMO** level in physical form it shall make arrangements for the Classified Information to be transmitted to the territory of the other Party through Government-to-Government channels or through other secure channels mutually approved by the NSAs or relevant CSAs of both Parties.
- (3) In cases of urgency, Classified Information at the **RISERVATISSIMO** level may be transmitted via a commercial courier company authorised by the Italian NSA.
- (4) If a Party transmits Classified Information at the **SEGRETISSIMO**, **UK TOP SECRET**, **SEGRETO**, **UK SECRET** or **RISERVATISSIMO** level in physical form it shall include with it a receipt for signature by or on behalf of the Receiving Party or recipient Contractor to be returned by the date specified in the receipt.
- (5) If a Party wishes to transmit Classified Information at the **RISERVATO** or **UK OFFICIAL-SENSITIVE** level in physical form it may be transmitted to the territory of the other Party by international postal services, by a commercial courier company, authorised personal hand carriage or through diplomatic channels.
- (6) In the case of physical transmission of a large consignment containing Classified Information, procedures for transportation as freight shall be jointly reviewed and agreed by the NSAs or relevant CSAs of both Parties.
- (7) In the case of physical transmission of Classified Information at the **SEGRETISSIMO**, **UK TOP SECRET**, **SEGRETO**, **UK SECRET** or **RISERVATISSIMO** level from the territory of one Party to the territory of the other Party by freight, the transport shall be jointly reviewed and agreed by the NSAs or relevant CSAs of both Parties. The NSA or relevant CSA of the consignor shall provide to the NSA or relevant CSA of the receiving Facility a transportation plan for approval prior to transportation commencing. The plan shall, as a minimum, include the following information:
  - a) the names and identification card/passport numbers of the relevant personnel involved in the transportation;

- b) the level and validity of the PSCs for all the relevant personnel directly involved in the transportation;
- c) if appropriate, confirmation of the transportation company's FSC;
- d) a list of the Classified Information to be transported by freight, including the Security Classification Levels of that information;
- e) details of the transport schedule, including departure time, expected time of delivery and possible stops and overnight stays; and
- f) details of the planned route, including details of the means of transportation to be used.

Deviations from the transportation plan are not permitted unless these are necessary due to the occurrence of unforeseen incidents.

- (8) If a Party wishes to provide Classified Information electronically it shall transmit it in encrypted form using cryptographic methods and means mutually accepted by the Parties.
- (9) As an exception to paragraph (8) of this Article, if a Party wishes to provide Classified Information electronically at the UK OFFICIAL-SENSITIVE level it may do so in clear text if suitable cryptographic methods and means are not available and if permitted by the relevant UK CSA. If not permitted, the Classified Information shall be protected by cryptographic methods and means that have been mutually accepted by the Parties. This paragraph does not apply to Classified Information at the SEGRETISSIMO, UK TOP SECRET, SEGRETO, UK SECRET, RISERVATISSIMO and RISERVATO level.

## **ARTICLE 9**

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

- (1) Reproductions and translations shall retain the Security Classification Level which was applied to the original and shall be protected in accordance with the provisions of this Agreement. Such reproductions and translations shall be limited to the minimum required and shall only be made by individuals who hold an appropriate level of PSC.
- (2) Translations shall contain a suitable annotation, in the language of translation, indicating that they contain Classified Information of the Providing Party.
- (3) Classified Information at the SEGRETISSIMO or UK TOP SECRET level shall be reproduced or translated only upon obtaining the prior written permission of the Providing Party.
- (4) Unless the Providing Party has given its prior written consent, Classified Information marked SEGRETISSIMO or UK TOP SECRET which is no longer required shall not be destroyed by the Receiving Party but returned to the Providing Party in accordance with Article 8 of this Agreement.
- (5) If no longer required, Classified Information marked SEGRETO, UK SECRET or RISERVATISSIMO shall be destroyed in accordance with the standards and methods which the Receiving Party would be required to apply to its Classified Information at the equivalent Security Classification Level. The Receiving Party shall inform the Providing Party of such destruction.
- (6) If no longer required, Classified Information marked RISERVATO or UK OFFICIAL-SENSITIVE shall be destroyed in accordance with the standards and methods which the Receiving Party would be required to apply to its Classified Information at the equivalent Security Classification Level.

- (7) If a crisis situation makes it impossible for the Receiving Party to protect or return Classified Information generated and/or provided by the Providing Party, the Classified Information shall be destroyed as soon as is practicable using any appropriate means in order to avoid a Security Incident. The NSA or relevant CSA of the Receiving Party shall inform the NSA or relevant CSA of the Providing Party in writing if Classified Information provided under this Agreement has been destroyed in such a situation.
- (8) The Providing Party may prohibit the reproduction, translation or destruction of its Classified Information by adding an appropriate marking, by attaching a written notice, or by providing handling instructions to the Receiving Party.

## **ARTICLE 10**

### **CLASSIFIED CONTRACTS AND FACILITY SECURITY CLEARANCES**

- (1) If a Party proposes to place a Classified Contract involving Classified Information at the **SEGRETISSIMO**, **UK TOP SECRET**, **SEGRETO**, **UK SECRET** or **RISERVATISSIMO** level with a Contractor under the jurisdiction of the other Party, the NSA or relevant CSA of the Party proposing the contract shall first obtain written confirmation from the NSA or relevant CSA of that Party that the Contractor under the jurisdiction of the other Party has been granted an FSC and/or PSC to at least the appropriate Security Classification Level.
- (2) The NSA or CSA which has granted a FSC or PSC shall be responsible, in accordance with its national laws and regulations, for monitoring the security conduct of the Contractor to which, or individual to whom, it applies.
- (3) For the purposes of this Agreement the Providing Party shall recognise FSCs issued by the NSA or CSA of the Receiving Party.
- (4) A Party entering or proposing to enter into a Classified Contract after the entry into force of this Agreement involving Classified Information at the **SEGRETISSIMO**, **UK TOP SECRET**, **SEGRETO**, **UK SECRET** or **RISERVATISSIMO** level shall ensure that the Contractor is legally obliged to afford the other Party's Classified Information it receives the same degree of protection as the Receiving Party is required to afford it under this Agreement.
- (5) A Party shall ensure that all Classified Contracts contain provisions that substantially reflect the relevant security requirements for the protection of Classified Information imposed on Parties by virtue of this Agreement. For Classified Contracts at the **SEGRETISSIMO**, **UK TOP SECRET**, **SEGRETO**, **UK SECRET** or **RISERVATISSIMO** level a copy of the Classified Contract shall be submitted to the NSA or relevant CSA of the Receiving Party to facilitate their security monitoring of the contract.
- (6) If the NSA or relevant CSA of the Receiving Party withdraws or downgrades an existing FSC issued to a Contractor Facility which handles or stores Classified Information generated and/or provided under this Agreement the NSA or relevant CSA of the Providing Party shall be informed as soon as is practicable.
- (7) If the Providing Party has a valid security reason to suspect that a Facility of a Contractor located in the territory of the other Party issued with a FSC is not adequately protecting its Classified Information the NSA of the Providing Party may request that a security inspection is carried out by the NSA or relevant CSA of the Receiving Party in order to monitor compliance.
- (8) An FSC is not required for Classified Contracts that are limited to Classified Information at the level of **RISERVATO** or **UK OFFICIAL-SENSITIVE**. A Party entering or proposing to enter into a Classified Contract after the entry into force of this Agreement concerning **RISERVATO** or **UK**

OFFICIAL-SENSITIVE Classified Information shall ensure that it contains an appropriate security requirements clause which shall define the minimum security requirements to be applied by the Contractor to Classified Information that is generated and/or provided as a result of the Contract. The security requirements clause should include a provision concerning the appointment, by the Contractor, of a person who has the overall responsibility for the protection of Classified Information marked RISERVATO or UK OFFICIAL-SENSITIVE.

## **ARTICLE 11 VISITS**

- (1) If an official of a Party is required to visit a government department, agency or establishment falling under the responsibility of the other Party, and this visit will or may involve access to Classified Information at the SEGRETISSIMO, UK TOP SECRET, SEGRETO, UK SECRET or RISERVATISSIMO level, the visitor shall ensure that details of their PSC are provided to the host prior to the visit.
- (2) If an official of a Party is required to visit a Facility of a Contractor which has been issued a FSC by the other Party, and this visit will or may involve access to Classified Information at the SEGRETISSIMO, UK TOP SECRET, SEGRETO, UK SECRET or RISERVATISSIMO level, the procedure as set out in paragraphs (3), (4) and (5) of this Article shall be followed.
- (3) A request for visit as referred to in paragraph (2) of this Article shall be submitted by the visitor's NSA or CSA to the NSA or relevant CSA of the host Facility at least 20 working days prior to the commencement of the visit. The request for visit shall include at least the following information:
  - a) the visitor's name, date and place of birth, nationality and identification card/passport number;
  - b) the visitor's official job title, with the name of the organisation the visitor represents;
  - c) the date and duration of the visit. In the case of recurring visits the total period covered by the visits shall be stated;
  - d) the purpose of the visit and subject(s) to be discussed;
  - e) the name, address, phone number, e-mail address and point of contact of the Facility to be visited;
  - f) an indication of the highest Security Classification Level of Classified Information to be discussed or accessed;
  - g) the level and validity of the visitor's PSC; and
  - h) a dated signature of a representative of the visitor's NSA or CSA (or person acting on their behalf) who is duly authorised to make such visit requests.
- (4) In urgent cases, the NSAs or relevant CSAs of both Parties may agree on a shorter timescale than that stated in paragraph (3) of this Article for the submission of the request for visit.
- (5) For specific Classified Contracts or programmes it may be possible, subject to the approval of the NSAs or relevant CSAs of both Parties, to establish a recurring visitor list. Such a list shall be valid for an initial period not exceeding twelve months from the date of authorisation and may be extended for further periods of time not exceeding twelve months subject to the mutual agreement of the NSAs or relevant CSAs. A recurring visitor list shall be submitted in accordance with paragraphs (3) and (4) of this Article. Once such a list has been authorised, visits may be

arranged directly between the visitor and the host Facility without the further involvement of the NSAs or relevant CSAs.

- (6) Visits shall only take place when the visit request as described in paragraphs (3), (4) and (5) of this Article has been authorised by the NSA or relevant CSA of the host Facility.
- (7) The NSAs or CSAs of both Parties may determine that alternative visit procedures to those described in paragraphs (3), (4), (5) and (6) of this Article may be adopted for specific Classified Contracts or programmes. Such alternative visit procedures shall be mutually agreed and may be documented in Programme Security Instructions.
- (8) Nothing in this Agreement affects visits conducted under the EDIR Framework Agreement.
- (9) Visits involving access to Classified Information at the level of RISERVATO or UK OFFICIAL-SENSITIVE shall be arranged directly between the visitor and the host Facility to be visited.

## **ARTICLE 12 SECURITY INCIDENTS**

- (1) Subject to paragraph (2) of this Article, any actual or suspected Security Incident occurring in the territory of a Party, or at a Facility for which a Party is responsible (including that Party's diplomatic mission), shall be investigated immediately by that Party.
- (2) If a Security Incident is confirmed by the investigating Party, that Party shall take appropriate measures in accordance with its applicable national laws and regulations to limit the consequences of the incident and prevent a recurrence.
- (3) If a Security Incident has resulted in the compromise of Classified Information, the NSA of the Party in whose territory the incident has occurred, or the NSA of the Party responsible for the Facility, shall inform the other NSA of the outcome of the investigation in writing as soon as possible and of any actions taken to prevent a recurrence.
- (4) If a Security Incident involving Classified Information occurs outside the territories of Italy or the UK, the responsible NSA or CSA shall take appropriate measures to limit the consequences of the Security Incident and inform the other NSA or relevant CSA of the incident as soon as is practicable.

## **ARTICLE 13 FINANCIAL MATTERS**

Each Party shall bear its own costs regarding the implementation of this Agreement without exceeding its ordinary budget availability.

## **ARTICLE 14 SETTLEMENT OF DISPUTES**

Any dispute or disagreement between the Parties on the interpretation or application of this Agreement shall be settled by means of consultation between the Parties and shall not be referred to a Third Party for resolution.

**ARTICLE 15**  
**FINAL PROVISIONS**

- (1) Each Party shall notify the other Party by the exchange of diplomatic notes once the internal legal procedures necessary for entry into force of this Agreement have been completed. This Agreement shall enter into force on the first day of the second month following the receipt of the later notification.
- (2) This Agreement shall be applied provisionally from the date of signature.
- (3) This Agreement may be amended at any time at the request of either Party. Agreed amendments shall enter into force on the first day of the second month following the exchange of diplomatic notes.
- (4) The NSAs or CSAs may conclude implementing arrangements pursuant to this Agreement.
- (5) This Agreement shall remain in force until further notice. Either Party may terminate this Agreement by submitting a diplomatic note to the other Party. In that case, this Agreement shall terminate six months after the notification is received by the other Party.
- (6) In case of termination of this Agreement, all Classified Information generated and/or provided by the Parties shall continue to be protected in accordance with the provisions set forth herein. If requested, such Classified Information shall be securely returned by the Receiving Party to the Providing Party.
- (7) After the entry into force of this Agreement, the Party in whose territory the Agreement is concluded shall take immediate measures so as to have this Agreement registered by the Secretariat of the United Nations in accordance with Article 102 of the UN Charter. That Party shall notify the other Party of the registration and of the registration number in the UN Treaty Series as soon as the UN Secretariat has issued it.
- (8) Upon the entry into force of this Agreement, the General Security Arrangement between the Government of the Italian Republic and the Government of the United Kingdom of Great Britain and Northern Ireland concerning the protection of classified information exchanged for the purposes of research, development, production and procurement between the two countries, dated 16 February 2004 as amended, shall be terminated. Any Classified Information generated and/or provided previously under that Arrangement shall be protected in accordance with the provisions of this Agreement.

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

Done in Rome on 22nd September 2020 in two original copies, in the Italian and English languages, each text being equally authentic.

**For the Government of the  
Italian Republic:**



**For the Government of the United  
Kingdom of Great Britain and  
Northern Ireland:**



