ACCORDO

TRA

IL GOVERNO DELLA REPUBBLICA ITALIANA

E

IL GOVERNO DEL GRANDUCATO DEL LUSSEMBURGO

SULLO

SCAMBIO E RECIPROCA PROTEZIONE

DELLE INFORMAZIONI CLASSIFICATE

Il Governo della Repubblica Italiana

e

il Governo del Granducato del Lussemburgo

qui di seguito denominati "Le Parti"

desiderando assicurare, in conformità con le proprie leggi e regolamenti nazionali, la protezione delle informazioni classificate scambiate tra le Parti o tra enti pubblici o privati sotto la propria giurisdizione, nel rispetto degli interessi nazionali e di sicurezza,

riconoscendo la necessità di stabilire comuni regole di sicurezza per la protezione delle informazioni classificate, anche in relazione alla possibilità dell'attuazione di accordi tecnici di cooperazione ed allo sviluppo di attività contrattuali tra le Parti,

hanno concordato quanto segue:

ARTICOLO 1
SCOPO

In conformità con le proprie leggi e regolamenti nazionali e nel rispetto degli interessi nazionali, di sicurezza e delle attività industriali, entrambe le Parti prendono provvedimenti idonei ad assicurare la protezione delle Informazioni Classificate prodotte o scambiate nel rispetto del presente Accordo.

ARTICOLO 2
DEFINIZIONI

Ai fini di questo Accordo questi termini hanno il seguente significato:

a) **Informazione Classificata:** Ogni informazione, a prescindere dalla forma in cui è prodotta o trasmessa tra le Parti, alla quale è stata assegnata una classifica di segretezza, in conformità con le leggi e i regolamenti nazionali delle Parti.

b) **Autorità Competente per la Sicurezza**: un ente competente, autorizzato in conformità alle leggi e regolamenti nazionali delle Parti, responsabile dell'attuazione del presente Accordo.

c) **Parte Originatrice**: la Parte, incluso ogni ente pubblico o privato sotto la propria giurisdizione, che rilascia Informazioni Classificate alla Parte Ricevente.

d) **Parte Ricevente**: la Parte, incluso ogni ente pubblico o privato sotto la propria giurisdizione, che riceve Informazioni Classificate dalla Parte Originatrice.

e) **Necessità di Conoscere**: un principio in base al quale l'accesso a Informazioni Classificate può essere autorizzato ad una persona solo in relazione ai propri incarichi ufficiali o ai propri compiti.

f) **Abilitazione di Sicurezza Personale**: Una positiva decisione adottata a seguito di una procedura di investigazione conforme alle leggi ed ai regolamenti nazionali, sulla base della quale una persona è autorizzata all'accesso ed alla trattazione di Informazioni Classificate fino al livello indicato nella decisione.

g) **Abilitazione di Sicurezza Industriale**: Una positiva decisione adottata a seguito di una procedura di investigazione, che attesti che un contraente è una persona giuridica idonea alla trattazione di Informazioni classificate in conformità con le leggi ed i regolamenti nazionali di una delle Parti.

h) **Contraente**: Un soggetto pubblico o privato che possiede la capacità giuridica di concludere contratti o subcontratti.

i) **Contratto Classificato**: Un contratto con un Contraente che contiene o implica la conoscenza di Informazioni Classificate.

j) **Parte Terza**: Uno Stato, incluso ogni soggetto pubblico o privato sotto la propria giurisdizione, o una organizzazione internazionale che non è Parte del presente Accordo.

k) **Visita**: L'accesso a soggetti pubblici o privati, per lo scopo di questo Accordo, che include l'accesso e la trattazione di Informazioni Classificate.

ARTICOLO 3
AUTORITÀ COMPETENTI PER LA SICUREZZA

(1) Le Autorità Competenti per la Sicurezza, nominate dalle Parti come responsabili per la generale applicazione e i relativi controlli riferiti a tutti gli aspetti di questo Accordo, sono:

nella Repubblica Italiana:

- *Presidenza del Consiglio dei Ministri - Autorità Nazionale per la Sicurezza - Dipartimento delle Informazioni per la Sicurezza (DIS) - UCSe.*

nel Governo del Granducato del Lussemburgo:

- *Service de Renseignement de l'Etat*
  Autorité nationale de Sécurité

(2) le Autorità Competenti per la Sicurezza devono notificare l'un l'altra di ogni altra Autorità di Sicurezza responsabile per l'attuazione del presente Accordo;

(3) le Parti devono informare l'un l'altra, attraverso canali diplomatici, di ogni successivo cambiamento delle Autorità Competenti per la Sicurezza;

(4) al fine di realizzare e mantenere criteri di sicurezza equivalenti, le Autorità Competenti per la Sicurezza devono, su richiesta, fornirsi reciprocamente informazioni circa i propri criteri, procedure e prassi di sicurezza nazionali per la protezione delle Informazioni Classificate. A tal fine le Autorità Competenti per la Sicurezza possono scambiarsi reciproche visite;

(5) le Autorità Competenti per la Sicurezza devono assicurare una rigorosa e vincolante osservanza a questo Accordo da parte di ogni ente pubblico o privato delle Parti, in conformità con le leggi ed i regolamenti nazionali.

ARTICOLO 4
CLASSIFICHE DI SEGRETEZZA

(1) Le Informazioni Classificate rilasciate in applicazione del presente Accordo devono essere contrassegnate con un adeguato livello di classifica, in conformità con le leggi ed i regolamenti nazionali delle Parti.

(2) I seguenti livelli di classifica di segretezza nazionale sono equivalenti:

Repubblica Italiana	**Granducato del Lussemburgo**
SEGRETISSIMO	TRES SECRET LUX
SEGRETO	SECRET LUX
RISERVATISSIMO	CONFIDENTIEL LUX
RISERVATO	RESTREINT LUX

ARTICOLO 5
PRINCIPI PER LA PROTEZIONE DELLE INFORMAZIONI CLASSIFICATE

(1) Le Parti assicurano, alle Informazioni Classificate cui si riferisce questo accordo, lo stesso grado di protezione previsto per le proprie Informazioni Classificate del corrispondente livello di classifica di segretezza.

(2) L'Autorità Competente per la Sicurezza della Parte Originatrice deve:
   a) assicurare che l'Informazione Classificata sia contrassegnata con adeguato livello di classifica di segretezza, in conformità con le proprie leggi e regolamenti nazionali, e
   b) informare la Parte Ricevente circa le condizioni di rilascio o delle limitazioni all'utilizzo dell'Informazione Classificata ed ogni successivo cambiamento nella classifica di segretezza.

(3) L'Autorità Competente per la Sicurezza della Parte Ricevente deve:
   a) assicurare che l'Informazione Classificata rechi i corrispondenti contrassegni di sicurezza in conformità con quanto previsto dal Paragrafo 2 dell'Articolo 4, e
   b) assicurare che il livello di classifica di segretezza non sia modificato senza l'autorizzazione scritta della Parte Originatrice;
   c) utilizzare l'Informazione Classificata solo per lo scopo per il quale è stata rilasciata e nei limiti stabiliti dalla Parte Originatrice;
   d) non rilasciare Informazioni Classificate ad una Parte Terza senza il previo consenso scritto della Parte Originatrice.

ARTICOLO 6

ACCESSO ALLE INFORMAZIONI CLASSIFICATE E ABILITAZIONI DI SICUREZZA PERSONALI

(1) L'accesso alle Informazioni Classificate al livello RISERVATISSIMO/ CONFIDENTIEL LUX e superiore è permesso solo a quelle persone che hanno necessità di conoscere, che sono in possesso di un'adeguata Abilitazione di Sicurezza Personale e che sono indottrinate regolarmente.

(2) L'accesso alle Informazioni Classificate al livello RISERVATO/ RESTREINT LUX è limitato a quelle persone che hanno necessità di conoscere e che sono state adeguatamente indottrinate.

(3) Le Parti riconoscono reciprocamente le rispettive Abilitazioni di Sicurezza Personali. Il paragrafo 2 dell'articolo 4 si applica conformemente.

(4) Su richiesta, le Autorità Competenti per la Sicurezza collaborano e forniscono reciproca assistenza durante le procedure di indagine per il rilascio delle Abilitazioni di Sicurezza Personali.

(5) Le Autorità Competenti per la Sicurezza si informano con sollecitudine, in forma reciproca, di ogni modifica nelle Abilitazioni di Sicurezza Personali reciprocamente riconosciute.

ARTICOLO 7

PROTEZIONE DELLE INFORMAZIONI CLASSIFICATE NEI SISTEMI INFORMATICI E DI TELECOMUNICAZIONE

(1) Ogni Parte assicura che siano applicate adeguate misure di sicurezza per la protezione di quelle Informazioni Classificate trattate, conservate o trasmesse con sistemi informatici e di telecomunicazioni. Tali misure garantiscono la riservatezza, l'integrità, la disponibilità e, ove applicabile, la non disconoscibilità e l'autenticità dell'Informazione Classificata nonché un adeguato livello di responsabilità e di tracciabilità delle azioni relative ad una determinata Informazione Classificata.

(2) A tal fine, le Parti assicurano che tali Informazioni Classificate scambiate sono conservate, gestite e protette in ottemperanza con le rispettive leggi e regolamenti nazionali.

(3) Entrambe le Parti riconoscono reciprocamente ogni atto formale di approvazione, riferito alle apparecchiature ed ai meccanismi relativi ai sistemi informatici e di telecomunicazione, emanato dalla rispettiva Autorità Competente per la Sicurezza.

(4) Ove necessario, un elenco aggiornato di tali apparecchiature e meccanismi approvati viene scambiato tra le Autorità Competenti per la Sicurezza.

ARTICOLO 8

TRASMISSIONE DELLE INFORMAZIONI CLASSIFICATE

(1) Le Informazioni Classificate sono trasmesse tra le Parti attraverso canali diplomatici o attraverso altri canali sicuri reciprocamente approvati dalle rispettive Competenti Autorità per la Sicurezza, in conformità con le proprie leggi e regolamenti nazionali.

(2) Le Informazioni Classificate "SEGRETISSIMO/TRES SECRET LUX" sono inviate solo attraverso canali diplomatici o militari in accordo con le leggi ed i regolamenti nazionali.

(3) Le Informazioni Classificate "RISERVATO/RESTREINT LUX" possono essere trasmesse anche attraverso la posta od un altro servizio di consegna in conformità con le leggi ed i regolamenti nazionali.

(4) Nel caso di trasmissione di una consegna voluminosa contenente Informazioni Classificate, le procedure per il trasporto sono valutate e concordate congiuntamente, caso per caso, dalle Autorità Competenti per la Sicurezza delle Parti.

ARTICOLO 9

RIPRODUZIONE, TRADUZIONE E DISTRUZIONE DELLE INFORMAZIONI CLASSIFICATE

(1) Tutte le riproduzioni e le traduzioni recano le adeguate classifiche di segretezza e sono protette nello stesso modo delle Informazioni Classificate originali. Le traduzioni ed il

numero delle riproduzioni devono essere limitate al minimo necessario per uno scopo ufficiale.

(2) Tutte le traduzioni sono contrassegnate con il livello di classifica originario e contengono un'adeguata annotazione, nella lingua di traduzione, ed attestante che contiene Informazioni Classificate della Parte Originatrice.

(3) Le Informazioni Classificate contrassegnate SEGRETISSIMO/TRES SECRET LUX, sia nella versione originale che in quella tradotta, sono riprodotte solo previo consenso scritto rilasciato dalla Parte Originatrice.

(4) Le Informazioni Classificate contrassegnate SEGRETISSIMO/TRES SECRET LUX non devono essere distrutte. L'informazione deve essere restituita alla Parte Originatrice dopo che non è più considerata necessaria dalla Parte Ricevente.

(5) Le Informazioni Classificate contrassegnate SEGRETO/SECRET LUX o di livello inferiore devono essere distrutte, in conformità con le rispettive leggi e regolamenti nazionali, non appena la Parte Ricevente non le reputi più necessarie. La Parte Ricevente informa la Parte Originatrice di tale distruzione.

(6) In una situazione di crisi in cui è impossibile proteggere o restituire le Informazioni Classificate trasmesse o generate nell'ambito di questo Accordo, le Informazioni Classificate devono essere distrutte immediatamente. La Parte Ricevente, non appena possibile, informa l'Autorità Competente per la Sicurezza della Parte Originatrice circa l'avvenuta distruzione.

ARTICOLO 10

CONTRATTI CLASSIFICATI E ABILITAZIONI DI SICUREZZA INDUSTRIALE

(1) Prima di rilasciare Informazioni Classificate relative ad un Contratto Classificato a Contraenti, subcontraenti o potenziali Contraenti, la Parte Ricevente assicura che:

a) tali Contraenti, subcontraenti o potenziali Contraenti e le rispettive infrastrutture possiedono la capacità di proteggere le Informazioni Classificate in modo adeguato, in conformità con le leggi ed i regolamenti nazionali;

b) i Contraenti, subcontraenti o i potenziali Contraenti e le loro infrastrutture sono in possesso di un'Abilitazione di Sicurezza Industriale di adeguato livello, in conformità con le leggi ed i regolamenti nazionali;

c) le persone che svolgono funzioni che richiedono l'accesso alle Informazioni Classificate sono in possesso di un'Abilitazione di Sicurezza Personale al livello adeguato, in conformità con le leggi ed i regolamenti nazionali;

d) tutte le persone che hanno accesso alle Informazioni Classificate sono informate delle proprie responsabilità ed obblighi concernenti la protezione di tali Informazioni, in conformità con le leggi ed i regolamenti nazionali della Parte Ricevente.

(2) Ogni Autorità Competente per la Sicurezza può richiedere all'Autorità Competente per la Sicurezza dell'altra Parte di effettuare una visita di valutazione sulla sicurezza di un'infrastruttura per assicurare una costante conformità con i livelli di sicurezza, in accordo con le leggi ed i regolamenti nazionali.

(3) Un Contratto Classificato deve contenere disposizioni sui requisiti di sicurezza, i livelli di classifica di ogni aspetto o elemento del Contratto Classificato e uno specifico riferimento a questo Accordo. Una copia di tale documento deve essere inviata alle Autorità Competenti per la Sicurezza delle Parti.

(4) Le Parti riconoscono reciprocamente le proprie Abilitazioni di Sicurezza Industriale.

(5) Le Autorità Competenti per la Sicurezza si informano prontamente l'un l'altra circa ogni modifica nelle Abilitazioni di Sicurezza Industriale reciprocamente riconosciute.

ARTICOLO 11

VISITE

(1) Le Visite che implicano l'accesso alle Informazioni Classificate sono soggette ad una preventiva autorizzazione dell'Autorità Competente per la Sicurezza della Parte ospitante.

(2) Una richiesta di visita deve essere inviata alla relativa Autorità Competente per la Sicurezza almeno 30 giorni prima dell'inizio della visita stessa. La richiesta di visita include i seguenti dati, che devono essere usati solo per lo scopo della visita:

a) il nome del visitatore, la data ed il luogo di nascita, la cittadinanza ed il numero della carta d'identità/passaporto;
b) l'incarico del visitatore, con l'indicazione dell'organizzazione che il visitatore rappresenta;
c) un'indicazione del progetto nel quale il visitatore è coinvolto;
d) la validità ed il livello dell'Abilitazione di Sicurezza Personale del visitatore, se richiesti;
e) il nome, l'indirizzo, il numero telefono/fax, l'e-mail del Funzionario alla sicurezza dell'infrastruttura che deve essere visitata;
f) lo scopo della visita, incluso il livello più alto di classifica dell'Informazione Classificata che deve essere trattata;
g) la data e la durata della visita. Nel caso di visite ricorrenti deve essere indicato il periodo complessivo riferito alle visite;
h) la data e la firma della Autorità Competente per la Sicurezza del visitatore.

(3) In casi urgenti, le Autorità Competenti per la Sicurezza possono concordare un periodo più breve per l'invio di una richiesta di visita.

(4) Le Autorità Competenti per la Sicurezza possono concordare una lista di visitatori autorizzati a svolgere visite ricorrenti. La lista è valida per un periodo iniziale che non ecceda i 12 mesi e può essere estesa per un ulteriore periodo di tempo non eccedente i 12 mesi. Una richiesta per le visite ricorrenti deve essere sottoposta in conformità con il paragrafo 2 di questo Articolo. Una volta che la lista è stata approvata, le visite possono essere direttamente concordate tra le infrastrutture coinvolte.

(5) Ogni Parte garantisce la protezione dei dati personali dei visitatori in accordo con le leggi ed i regolamenti nazionali.

ARTICOLO 12

VIOLAZIONI ALLA SICUREZZA

(1) Nel caso di una violazione alla sicurezza che risulta da una non autorizzata divulgazione, da un'appropriazione indebita, da una perdita, o sospetta compromissione, di Informazioni Classificate, l'Autorità Competente per la Sicurezza della Parte Ricevente informa immediatamente di ciò, per iscritto, l'Autorità Competente per la Sicurezza della Parte Originatrice.

(2) La Parte competente adotta tutte le misure previste dalle leggi e dai regolamenti nazionali, al fine di limitare le conseguenze della violazione, come riferite nel Paragrafo 1 dell'articolo e al fine di prevenire ulteriori violazioni. Su richiesta, l'altra Parte fornisce un'assistenza adeguata; la suddetta Parte sarà informata degli esiti dei procedimenti e delle misure adottate a causa della violazione.

(3) Quando la violazione alla sicurezza è avvenuta presso una Parte Terza, l'Autorità Competente per la Sicurezza della Parte che ha inviato l'Informazione Classificata deve eseguire, appena possibile, le azioni previste nel paragrafo 2 di questo Articolo.

(4) Le Autorità Competenti per la Sicurezza si informano reciprocamente sui rischi eccezionali riguardanti la sicurezza che possono pregiudicare l' Informazione Classificata rilasciata.

ARTICOLO 13

SPESE

(1) L'esecuzione di questo Accordo non comporta alcun costo.

(2) Nel caso in cui, nel corso dell'esecuzione di questo Accordo, sopravvengano costi imprevisti per ciascuna delle Parti, ogni Parte deve sostenere le proprie spese.

ARTICOLO 14

RISOLUZIONE DELLE CONTROVERSIE

Qualsiasi controversia che riguarda l'interpretazione o l'applicazione di questo Accordo deve essere definita attraverso consultazioni e negoziazioni tra le Parti. Nel frattempo, le Parti continuano ad ottemperare alle previsioni stabilite in questo Accordo.

ARTICOLO 15

DISPOSIZIONI FINALI

(1) Questo Accordo entra in vigore il primo giorno del secondo mese dalla data di avvenuta ricezione dell'ultima comunicazione scritta con la quale le Parti si sono informate reciprocamente, attraverso i canali diplomatici, che le loro procedure legali interne necessarie per la rispettiva entrata in vigore sono state completate.

(2) Questo accordo può essere emendato attraverso un reciproco consenso scritto tra le Parti. Gli emendamenti entrano in vigore in conformità con il paragrafo 1 di questo Articolo.

(3) Questo Accordo è concluso per un periodo di tempo indefinito. Ciascuna Parte può denunciare questo Accordo dando notizia all'altra Parte per iscritto attraverso canali diplomatici. In tal caso, questo Accordo termina sei mesi dopo la data nella quale l'altra Parte ha ricevuto la notizia di denuncia.

(4) Nel caso di rescissione di questo Accordo, tutte le Informazioni Classificate trasferite in osservanza di questo Accordo devono continuare ad essere protette in conformità con le previsioni qui stabilite e, dietro richiesta, restituite alla Parte Originatrice.

(5) Accordi attuativi possono essere conclusi per l'esecuzione di questo Accordo.

In fede di che, i sottoscritti, debitamente autorizzati hanno firmato il presente Accordo.
Fatto a Roma il 20 Aprile 2017 in tre originali in lingua italiana francese, e inglese, i testi in lingua italiana e francese sono autentici. Nel caso di qualsiasi divergenza sull'interpretazione, il testo in lingua inglese prevarrà.

In rappresentanza del Governo della Repubblica Italiana

In rappresentanza del Governo del Granducato del Lussemburgo

ACCORD

ENTRE

LE GOUVERNEMENT DE LA RÉPUBLIQUE D'ITALIE

ET

LE GOUVERNEMENT DU GRAND-DUCHÉ DE LUXEMBOURG

CONCERNANT

L'ÉCHANGE ET LA PROTECTION RÉCIPROQUE

D'INFORMATIONS CLASSIFIÉES

Le Gouvernement de la République d'Italie
et
le Gouvernement du Grand-Duché de Luxembourg

ci-après dénommés les « Parties »,

Désireux de garantir la protection des Informations classifiées échangées entre les Parties ou entre les entités publiques ou privées relevant de leur juridiction, dans le respect de la sécurité et des intérêts nationaux,

reconnaissant la nécessité d'établir des règlementations de sécurité communes pour la protection des Informations classifiées, également en ce qui concerne la possible mise en œuvre d'accords de coopération technique et le développement d'activités contractuelles entre les Parties,

conviennent ce qui suit :

ARTICLE 1
OBJECTIF

Les deux parties prendront des mesures appropriées, en conformité avec leurs législations et règlementations nationales respectives et dans le respect des intérêts nationaux, de la sécurité ainsi que des activités industrielles, afin de protéger les Informations classifiées qui seront transmises ou générées conformément au présent Accord.

ARTICLE 2
DÉFINITIONS

Aux fins du présent Accord, il faut entendre par :

a) **Information classifiée** : toute information, sous quelque forme que ce soit, transmise ou générée entre les Parties, faisant partie de la classification de sécurité conformément aux législations et règlementations nationales des Parties.

b) **Autorité de sécurité compétente** : tout organe compétent autorisé conformément aux lois et réglementations nationales des Parties, en charge de l'application du présent Accord.

c) **Partie d'origine :** la Partie, y compris les entités publiques ou privées relevant de la juridiction de cette dernière, qui transmet des Informations classifiées à la Partie destinataire.

d) **Partie destinataire :** la Partie, y compris les entités publiques ou privées relevant de la juridiction de cette dernière, qui reçoit des Informations classifiées de la Partie d'origine.

e) **Besoin d'en connaître** : le principe par lequel l'accès à toute Information classifiée ne peut être accordé à une personne que dans le cadre de sa fonction ou mission officielle.

f) **Habilitation de sécurité individuelle :** une décision positive prise suite à une procédure d'évaluation conformément aux législations et règlementations nationales, qui confère à une personne donnée l'accès à des Informations classifiées et l'autorise à traiter celles-ci jusqu'au niveau défini dans la décision.

g) **Habilitation de sécurité d'établissement :** une décision positive prise suite à une procédure d'évaluation qui certifie qu'un contractant satisfait aux conditions de traitement d'Informations classifiées conformément aux législations et règlementations nationales de l'une des parties.

h) **Contractant :** toute entité publique ou privée dotée de la capacité juridique de conclure des contrats ou des contrats de sous-traitance.

i) **Contrat classifié :** un contrat conclu avec un contractant qui contient ou implique la connaissance d'Informations classifiées.

j) **Tierce partie** : tout État, y compris les entités publiques et privées relevant de la juridiction de ce dernier, ou toute organisation internationale, qui n'est pas l'une des Parties au présent Accord.

k) **Visite :** accès à des entités publiques ou privées, dans le cadre du présent Accord, qui comprend l'accès à des Informations classifiées et le traitement de ces dernières

ARTICLE 3
AUTORITÉS DE SÉCURITÉ COMPÉTENTES

(1) Les autorités de sécurité compétentes désignées par les Parties en tant que responsables de l'application générale et de la supervision pertinente de l'ensemble des aspects du présent Accord, sont :

Pour la République d'Italie :
– Presidenza del Consiglio dei Ministri - Autorità Nazionale per la Sicurezza - Dipartimento delle Informazioni per la Sicurezza (DIS) - UCSe.

Pour le Grand-Duché de Luxembourg :
Service de Renseignement de l'État
Autorité nationale de Sécurité

(2) Les autorités de sécurité compétentes se tiennent mutuellement informées de toute autre autorité de sécurité compétente en charge de l'application du présent Accord.

(3) Les Parties se tiennent mutuellement informées, par la voie diplomatique, de toute modification apportée aux autorités de sécurité compétentes.

(4) En vue d'appliquer et de conserver des normes de sécurité similaires, les autorités de sécurité compétentes se tiennent, sur demande, mutuellement informées des normes, procédures et pratiques de sécurité nationales qu'elles appliquent en matière de protection d'Informations classifiées. À cette fin, les autorités de sécurité compétentes peuvent effectuer des visites réciproques.

(5) Les autorités de sécurité compétentes veilleront au respect strict et contraignant du présent Accord par toute entité publique ou privée des Parties conformément à leurs législations et règlementations nationales respectives.

ARTICLE 4
NIVEAUX DE SÉCURITÉ

(1) Toute Information classifiée délivrée en vertu du présent Accord est désignée par un niveau de sécurité approprié conformément aux lois et réglementations nationales des Parties.

(2) Les désignations nationales de classification de sécurité ci-après sont équivalentes :

République d'Italie	**Grand-Duché de Luxembourg**
SEGRETISSIMO	TRÈS SECRET LUX
SEGRETO	SECRET LUX
RISERVATISSIMO	CONFIDENTIEL LUX

ARTICLE 5

PRINCIPES POUR LA PROTECTION D'INFORMATIONS CLASSIFIÉES

(1) Les Parties accordent aux Informations classifiées visées dans le présent Accord la même protection que celle accordée à leurs propres Informations classifiées de niveau de sécurité correspondant.

(2) L'autorité de sécurité compétente de la Partie d'origine s'engage à :

a) s'assurer que les Informations classifiées sont désignées par un niveau de sécurité approprié, conformément aux lois et réglementations nationales ;
b) informer la Partie destinataire de toute condition de transmission ou de toute limite applicable à l'utilisation des Informations classifiées, et de toute modification ultérieure en matière de classification de sécurité.

(3) L'autorité de sécurité compétente de la Partie destinataire s'engage à :

a) s'assurer que les Informations classifiées sont désignées par un niveau de sécurité équivalent, conformément au paragraphe 2 de l'article 4 ; et
b) s'assurer que les niveaux de sécurité ne sont pas modifiés, excepté la présence d'une autorisation écrite de la Partie d'origine ;
c) utiliser les Informations classifiées uniquement aux fins pour lesquelles elles ont été délivrées et dans les limites fixées par la Partie d'origine ;
d) ne délivrer aucune Information classifiée à une tierce partie sans l'accord écrit de la Partie d'origine.

ARTICLE 6

ACCÈS À DES INFORMATIONS CLASSIFIÉES ET HABILITATIONS DE SÉCURITÉ INDIVIDUELLES

(1) L'accès à des Informations classifiées désignées comme RISERVATISSIMO/CONFIDENTIEL LUX ou de niveau supérieur est strictement réservé à des personnes ayant un « besoin de savoir », une habilitation de sécurité individuelle appropriée et recevant régulièrement des informations pertinentes.

(2) L'accès à des Informations classifiées RISERVATO/RESTREINT LUX est strictement réservé à des personnes ayant un « besoin de savoir » et qui ont été dûment informées en la matière.

(3) Les Parties reconnaissent mutuellement leurs habilitations de sécurité respectives. Le paragraphe 2 de l'article 4 s'applique en conséquence.

(4) Sur demande, les autorités de sécurité compétentes coopéreront et s'aideront mutuellement lors des procédures d'évaluation pour la délivrance d'habilitations de sécurité individuelles.

(5) Les autorités de sécurité compétentes s'informeront sans délai mutuellement, par écrit, de toute modification apportées aux habilitations de sécurité individuelles mutuellement reconnues.

ARTICLE 7

PROTECTION D'INFORMATIONS CLASSIFIÉES DANS LES SYSTÈMES DE COMMUNICATION ET D'INFORMATION

(1) Chacune des Parties veillera à la mise en œuvre de mesures appropriées en vue de protéger des Informations classifiées lors de leur traitement, stockage ou transmission via des systèmes de communication et d'information. Ces mesures devront garantir la confidentialité, l'intégrité, la disponibilité

et, le cas échéant, le non-rejet et l'authenticité des Informations classifiées ainsi qu'un niveau approprié de responsabilité et de traçabilité de toute action liée à ces Informations classifiées.

(2) A cette fin, les Parties s'assureront que de telles Informations classifiées échangées seront stockées, traitées et sauvegardées conformément à leurs dispositions et règlementations nationales respectives.

(3) Les deux Parties s'engagent à reconnaître mutuellement tout acte d'approbation formelle relatif à des équipements et mécanismes de systèmes de communication et d'information délivré par l'autorité de sécurité compétente en la matière.

(4) En cas de besoin, la liste actualisée de tels équipements et mécanismes approuvés sera transmise à l'autre autorité de sécurité compétente.

ARTICLE 8

TRANSMISSION D'INFORMATIONS CLASSIFIÉES

(1) Les Informations classifiées seront transmises entre les Parties par les voies diplomatiques ou d'autres canaux sécurisés approuvés par les autorités de sécurité compétentes conformément à leurs législations et règlementations nationales.

(2) Des Informations classifiées désignées « SEGRETISSIMO/TRES SECRET LUX » transiteront exclusivement par les voies diplomatiques ou militaires conformément aux législations et règlementations nationales.

(3) Des Informations classifiées désignées RISERVATO/RESTREINT LUX peuvent également être transmises par la voie postale ou un autre service de messagerie conformément aux législations et règlementations nationales.

(4) Lorsque la transmission porte sur un envoi de grand volume qui comprend des Informations classifiées, les procédures de ce transport seront convenues et appréciées, au cas par cas, par les autorités de sécurité compétentes des deux Parties.

ARTICLE 9

REPRODUCTION, TRADUCTION ET DESTRUCTION D'INFORMATIONS CLASSIFIÉES

(1) Toutes les reproductions et traductions portent un niveau de sécurité approprié et bénéficient du même degré de protection que les Informations classifiées originales. Les traductions et le nombre de reproductions est limité au minimum requis pour un usage officiel.

(2) Toutes les traductions porteront la même désignation du niveau de sécurité que l'original et incluront une note appropriée, dans la langue de traduction, indiquant qu'elles contiennent des Informations classifiées de la Partie d'origine.

(3) La traduction ou la reproduction d'Informations classifiées SEGRETISSIMO/TRES SECRET LUX n'est autorisée par la Partie d'origine.

(4) Les Informations classifiées SEGRETISSIMO/TRES SECRET LUX ne sont pas détruites, mais renvoyées à la Partie d'origine dès lors que la Partie destinataire n'en a plus l'utilité.

(5) Les Informations classifiées SEGRETO/SECRET LUX ou d'un niveau inférieur seront détruites conformément aux législations et règlementations nationales dès lors que la Partie destinataire n'en a plus l'utilité. La Partie destinataire informera la Partie d'origine de la destruction, le cas échéant.

(6) Dans le cas d'une situation de crise empêchant de protéger ou de retourner des Informations classifiées visées par le présent Accord, les Informations classifiées sont détruites immédiatement. La Partie destinataire avise dès que possible l'autorité sécurité compétente de la Partie d'origine d'une telle destruction.

ARTICLE 10

CONTRATS CLASSIFIÉS ET HABILITATIONS DE SÉCURITÉ D'ÉTABLISSEMENT

(1) Avant de fournir des Informations classifiées relatives à un contrat classifié à des contractants, sous-contractants ou contractants potentiel, la Partie destinataire doit s'assurer que :

a) les contractants, sous-contractants ou contractants potentiels et leurs établissements respectifs ont la capacité de garantir une protection appropriée des informations, conformément aux législations et règlementations nationales ;

b) les contractants, sous-contractants ou contractants potentiels et leurs établissements respectifs sont titulaires d'une habilitation de sécurité d'établissement du niveau adéquat, conformément aux législations et règlementations nationales;

c) les personnes qui exécutent des tâches qui requièrent l'accès à des Informations classifiées sont titulaires d'une habilitation de sécurité individuelle adaptée, conformément aux législations et règlementations nationales ;

d) toutes les personnes qui ont accès à des Informations classifiées sont informées de leurs responsabilités et obligations en matière de protection des informations conformément aux lois et réglementations de la Partie destinataire.

(2) Chacune des autorités de sécurité compétentes peut exiger une visite d'évaluation de sécurité par l'autorité de sécurité compétente de l'autre Partie dans un établissement afin de s'assurer que celui-ci est toujours conforme aux normes de sécurité conformément aux législations et règlementations nationales.

(3) Tout contrat classifié devra comporter des clauses qui précisent les exigences en matière de sécurité, la classification de chaque aspect ou élément du contrat classifié et référence spécifique au présent Accord. Une copie de ces dispositions sera transmise aux autorités de sécurité compétentes des Parties.

(4) Les Parties reconnaissent mutuellement leurs habilitations de sécurité d'établissement respectives.

(5) Les autorités de sécurité compétentes s'informeront sans délai mutuellement, par écrit, de toute modification apportées aux habilitations de sécurité d'établissement mutuellement reconnues.

ARTICLE 11

VISITES

(1) Les visites impliquant l'accès à des Informations classifiées sont soumises à l'autorisation préalable de l'autorité de sécurité compétente de la Partie hôte.

(2) Toute demande de visite est présentée à l'autorité de sécurité compétente au moins 30 jours avant le début de la visite, et contient les renseignements suivants : La demande de visite devra contenir les renseignements suivants, qui serviront exclusivement pour la visite concernée ;

a) nom, date et lieu de naissance, nationalité et numéro du passeport ou de la carte d'identité du visiteur ;

b) qualité du visiteur et descriptif de l'employeur que le visiteur représente ;

c) descriptif du projet auquel le visiteur participe ;

d) validité et niveau de l'habilitation de sécurité individuelle du visiteur, si nécessaire;

e) nom, adresse, numéro de téléphone/fax et adresse électronique de l'officier de sécurité de l'établissement à visiter ;

f) objet de la visite, avec mention du niveau de sécurité le plus élevé des Informations classifiées impliquées ;

g) date et durée de la visite. Dans le cas de visites récurrentes, il convient d'indiquer la période totale couverte par les visites ;

h) la date et la signature de l'autorité de sécurité compétente ayant missionné le visiteur.

(3) En cas d'urgence, les autorités de sécurité compétentes peuvent accorder un délai plus court pour la présentation d'une demande de visite.

(4) Les autorités de sécurité compétentes peuvent convenir d'établir une liste des visiteurs autorisés à effectuer des visites récurrentes. Cette liste est valable pour une première période maximale de 12 mois, qui peut être prolongée pour une nouvelle période maximale de 12 mois. Toute demande de visites récurrentes est présentée conformément au paragraphe 2 du présent article. Une fois la liste approuvée, les visites peuvent être organisées directement par les établissements concernés.

(5) Chacune des Parties garantit la protection des données personnelles des visiteurs conformément aux lois et réglementations nationales.

ARTICLE 12
INFRACTION À LA SÉCURITÉ

(1) En cas de perte ou de divulgation non autorisée d'Informations classifiées, avérée ou suspectée, l'autorité de sécurité compétente de la Partie destinataire en informe immédiatement par écrit l'autorité de sécurité compétente de la Partie d'origine.

(2) L'autorité compétente concernée prendra toutes les mesures appropriées possibles, conformément à ses lois et réglementations nationales, afin de limiter les conséquences de toute infraction telle que définie au paragraphe 1 du présent article, ou d'empêcher toute violation ultérieure. Sur demande, l'autre Partie participe à l'enquête ; elle est tenue informée du résultat de cette dernière et des mesures correctives entreprises à la suite de la violation.

(3) Au cas où la violation est le fait d'une partie tierce, l'autorité de sécurité compétente de la Partie ayant missionné le visiteur prendra sans délai les mesures précisées dans le paragraphe 2 de cet article.

(4) Les autorités de sécurité compétentes se tiennent mutuellement informées des risques de sécurité exceptionnels susceptibles de mettre en péril les Informations classifiées délivrées.

ARTICLE 13
Dépenses

(1) La mise en œuvre du présent Accord n'entraîne aucun frais.

(2) Au cas où dans le cadre de la mise en œuvre du présent accord des frais imprévus devraient concerner l'une ou l'autre des Parties, chacune assumera les dépenses qui la concernent.

ARTICLE 14
REGLEMENT DES LITIGES

Tout litige quant à l'interprétation ou l'application du présent Accord est exclusivement résolu par voie de consultation et négociation entre les Parties. Dans l'attente de l'accord amiable, les Parties continueront à exécuter leurs obligations découlant du présent Accord.

ARTICLE 15

DISPOSITIONS FINALES

(1) Le présent Accord est conclu pour une durée indéterminée et prend effet le premier jour du deuxième mois qui suit la réception de la dernière des notifications écrites par lesquelles les Parties se sont tenues mutuellement informées, par la voie diplomatique, de l'accomplissement des exigences légales internes requises pour son entrée en vigueur.

(2) Le présent Accord peut être modifié d'un commun accord par écrit entre les Parties. Ces modifications entrent en vigueur conformément aux dispositions du paragraphe 1 du présent article.

(3) Le présent Accord est conclu pour une durée indéterminée. Chaque Partie pourra mettre fin au présent Accord en prévenant l'autre Partie par écrit via les voies diplomatiques. Dans un tel cas, l'Accord prendra fin six mois à partir de la date de réception de la résiliation par l'autre Partie.

(4) Au cas où l'Accord sera résilié, toutes les Informations classifiées transmises dans le cadre du présent Accord continueront a rester sous protection conformément aux clauses des présentes et seront, sur demande, retournées à la Partie d'origine.

(5) Des modalités d'application peuvent être convenues dans le cadre de l'application du présent Accord.

En foi de quoi, les soussignés, dûment autorisés, ont signé le présent Accord.

Fait à Rome le 20 avril 2017 en [trois] exemplaires en langue italienne, française et anglaise, les textes français et italien étant considérés à égalité comme authentiques. Dans le cas d'un désaccord quant à l'interprétation des dispositions du présent Accord, le texte anglais prévaut.

Pour le Gouvernement de la République d'Italie

Pour le Gouvernement du Grand-Duché de Luxembourg

AGREEMENT

BETWEEN

THE GOVERNMENT OF THE ITALIAN REPUBLIC

AND

THE GOVERNMENT OF THE GRAND DUCHY OF LUXEMBURG

ON

THE EXCHANGE AND MUTUAL PROTECTION

OF CLASSIFIED INFORMATION

The Government of the Italian Republic
and
the Government of the Grand Duchy of Luxemburg

hereinafter referred to as the "Parties",

wishing to ensure the protection of Classified Information in accordance with their national laws and regulations exchanged between the Parties or between public and private entities under their jurisdiction, in respect of national interests and security,

recognising the need to establish common security regulations for the protection of Classified Information, also in relation to the possibility of implementing technical cooperation agreements and developing contractual activities between the Parties,

have agreed on the following:

ARTICLE 1

OBJECTIVE

In accordance with their national laws and regulations and in respect of national interests and security as well as of industrial activities both Parties shall take all appropriate measures to ensure the protection of Classified Information, which is transmitted or generated according to this Agreement.

ARTICLE 2

DEFINITIONS

For the purposes of this Agreement these terms mean the following:

a) **Classified Information**: Any information, regardless of its form, transmitted or generated between the Parties, to which a security classification has been assigned in accordance with the national laws and regulations of the Parties.

b) **Competent Security Authority**: A competent entity authorised according to the national laws and regulations of the Parties that is responsible for the implementation of this Agreement.

c) **Originating Party:** The Party, including any public or private entity under its jurisdiction, which releases Classified Information to the Recipient Party.

d) **Recipient Party:** The Party, including any public or private entity under its jurisdiction, which receives Classified Information from the Originating Party.

e) **Need-to-Know**: A principle by which access to Classified Information may be granted to an individual only in connection with his official duties or tasks.

f) **Personnel Security Clearance:** A positive decision following a vetting procedure in accordance with the national laws and regulations, on the basis of which an individual is authorised to have access to and to handle Classified Information up to the level defined in the decision.

g) **Facility Security Clearance:** A positive decision following a vetting procedure certifying that a contractor which is a legal entity fulfils the conditions of handling Classified Information in accordance with the national laws and regulations of one of the Parties.

h) **Contractor:** A public or private entity possessing the legal capacity to conclude contracts or subcontracts.

i) **Classified Contract:** A contract with a Contractor which contains or implies the knowledge of Classified Information.

j) **Third Party**: A state, including any public or private entity under its jurisdiction, or an international organisation that is not a Party to this Agreement.

k) **Visit**: Access to public or private entities, for the purpose of this Agreement, which includes access to and handling of Classified Information.

ARTICLE 3

COMPETENT SECURITY AUTHORITIES

(1) The Competent Security Authorities designated by the Parties as responsible for the general implementation and the relevant controls of all aspects of this Agreement are:

In the Italian Republic:
Presidenza del Consiglio dei Ministri - Autorità Nazionale per la Sicurezza - Dipartimento delle Informazioni per la Sicurezza (DIS) - UCSe.

In the Grand Duchy of Luxemburg:
Service de Renseignement de l'Etat
Autorité nationale de Sécurité

(2) The Competent Security Authorities shall notify each other of any other Competent Security Authorities that are responsible for the implementation of this Agreement.

(3) The Parties shall inform each other through diplomatic channels of any subsequent changes of the Competent Security Authorities.

(4) In order to achieve and maintain comparable standards of security, the Competent Security Authorities shall, on request, provide each other with information about their national security standards, procedures and practices for the protection of Classified Information. To this aim the Competent Security Authorities may visit each other.

(5) The Competent Security Authorities shall ensure a strict and binding observance of this Agreement by any public and private entity of the Parties in accordance with their national laws and regulations.

ARTICLE 4

SECURITY CLASSIFICATIONS

(1) Classified Information released under this Agreement shall be marked with the appropriate security classification level in accordance with the national laws and regulations of the Parties.

(2) The following national security classification markings are equivalent:

Italian Republic	**Grand Duchy of Luxemburg**
SEGRETISSIMO	TRES SECRET LUX
SEGRETO	SECRET LUX
RISERVATISSIMO	CONFIDENTIEL LUX
RISERVATO	RESTREINT LUX

ARTICLE 5

PRINCIPLES FOR THE PROTECTION OF CLASSIFIED INFORMATION

(1) The Parties shall afford to Classified Information referred to in this Agreement the same protection as to their own Classified Information of the corresponding security classification level.

(2) The Competent Security Authority of the Originating Party shall:

a) ensure that the Classified Information is marked with an appropriate security classification marking in accordance with its national laws and regulations, and
b) inform the Recipient Party of any conditions of release or limitations on the use of the Classified Information and of any subsequent changes in the security classification.

(3) The Competent Security Authority of the Recipient Party shall:

a) ensure that the Classified Information is marked with an equivalent security classification marking in accordance with Paragraph 2 of Article 4, and
b) ensure that the security classification level is not changed unless authorized in writing by the Originating Party;
c) use Classified Information only for the purpose for which it has been released and within the limitations stated by the Originating Party;
d) not release Classified Information to a Third Party without a prior written consent of the Originating Party.

ARTICLE 6

ACCESS TO CLASSIFIED INFORMATION AND PERSONNEL SECURITY CLEARANCES

(1) Access to Classified Information classified as RISERVATISSIMO/CONFIDENTIEL LUX and above shall be allowed only to those individuals with a Need-to-Know who hold appropriate Personnel Security Clearance and are regularly briefed.

(2) Access to Classified Information classified as RISERVATO/RESTREINT LUX shall be limited to persons who have a Need-to-know and who have been briefed accordingly.

(3) The Parties shall mutually recognise their Personnel Security Clearances. Paragraph 2 of Article 4 shall apply accordingly.

(4) On request, the Competent Security Authorities shall cooperate and give mutual assistance during the vetting procedures for the release of Personnel Security Clearances.

(5) The Competent Security Authorities shall promptly inform each other of any changes in mutually recognised Personnel Security Clearances.

ARTICLE 7
PROTECTION OF CLASSIFIED INFORMATION IN COMMUNICATION AND INFORMATION SYSTEMS

(1) Each Party shall ensure that appropriate measures are implemented for the protection of Classified Information processed, stored or transmitted in communication and information systems. Such measures shall ensure the confidentiality, integrity, availability and, where applicable, non-repudiation and authenticity of Classified Information as well as an

appropriate level of accountability and traceability of actions in relation to that Classified Information.

(2) To this end, the Parties shall ensure that such Classified Information exchanged will be stored, handled, and safeguarded in accordance with their respective national rules and regulations.

(3) Both Parties mutually recognize each formal act of approval, referring to equipment and mechanisms related to communication and information systems, issued by the relevant Competent Security Authority.

(4) When necessary, the updated list of such approved equipment and mechanisms shall be exchanged between the Competent Security Authorities.

ARTICLE 8

TRANSMISSION OF CLASSIFIED INFORMATION

(1) Classified Information shall be transmitted between the Parties through diplomatic channels or through other secure channels mutually approved by their Competent Security Authorities in accordance with the national laws and regulations.

(2) Information classified "SEGRETISSIMO/TRES SECRET LUX" shall be sent only through diplomatic or military channels in accordance with national laws and regulations.

(3) Information classified as RISERVATO/RESTREINT LUX may be transmitted also by post or another delivery service in accordance with national laws and regulations.

(4) In case of transmitting a large consignment containing Classified Information, procedures for transport shall be jointly agreed and evaluated, on a case-by-case basis, by the Competent Security Authorities of the Parties.

ARTICLE 9
REPRODUCTION, TRANSLATION AND DESTRUCTION OF CLASSIFIED INFORMATION

(1) All reproductions and translations shall bear appropriate security classification markings and shall be protected as the original Classified Information. The translations and the number of reproductions shall be limited to the minimum required for an official purpose.

(2) All translations shall be marked with the original security classification marking and shall contain a suitable annotation, in the language of translation, indicating that they contain Classified Information of the Originating Party.

(3) Classified Information marked SEGRETISSIMO/TRES SECRET LUX, both original and translation, shall be reproduced only upon prior written permission of the Originating Party.

(4) Classified Information marked SEGRETISSIMO/TRES SECRET LUX shall not be destroyed. It shall be returned to the Originating Party after it is no longer considered necessary by the Recipient Party.

(5) Information classified as SEGRETO/SECRET LUX or below shall be destroyed in accordance with relevant national laws and regulations after it is no longer considered necessary by the Recipient Party. The Recipient Party shall inform the Originating Party of such destruction.

(6) In a crisis situation in which it is impossible to protect or return Classified Information transmitted or generated under this Agreement, the Classified Information shall be destroyed immediately. The Recipient Party shall inform the Competent Security Authority of the Originating Party about this destruction as soon as possible.

ARTICLE 10

CLASSIFIED CONTRACTS AND FACILITY SECURITY CLEARANCES

(1) Before providing Classified Information related to a Classified Contract to Contractors, subcontractors or prospective Contractors, the Recipient Party shall ensure that:

a) such Contractors, subcontractors or prospective Contractors and their facilities have the capability to protect Classified Information adequately in accordance with national laws and regulations;

b) Contractors, subcontractors or prospective Contractors and their facilities hold an appropriate Facility Security Clearance at the adequate level, in accordance with national laws and regulations;

c) persons who perform functions which require access to Classified Information hold an appropriate Personnel Security Clearance in accordance with national laws and regulations;

d) all persons having access to Classified Information are informed of their responsibilities and obligations to protect such Information in accordance with national laws and regulations of the Recipient Party.

(2) Each Competent Security Authority may request that a security assessment visit is carried out at a facility by the Competent Security Authority of the other Party to ensure continuing compliance with security standards in accordance with national laws and regulations.

(3) A Classified Contract shall contain provisions on the security requirements, classification of each aspect or element of the Classified Contract and specific reference to this Agreement. A copy of such document shall be submitted to the Competent Security Authorities of the Parties.

(4) The Parties shall mutually recognise their Facility Security Clearances.

(5) The Competent Security Authorities shall promptly inform each other about any changes in mutually recognized Facility Security Clearances.

ARTICLE 11

VISITS

(1) Visits involving access to Classified Information shall be subject to prior permission of the Competent Security Authority of the host Party.

(2) A request for visit shall be submitted to the relevant Competent Security Authority at least 30 days prior to the commencement of the visit. The request for visit shall include the following data that shall be used for the purpose of the visit only:

a) the visitor's name, date and place of birth, citizenship and identification card/passport number;

b) the visitor's position, with a specification of the employer which the visitor represents;

c) a specification of the project in which the visitor participates;

d) the validity and level of the visitor's Personnel Security Clearance, if required;

e) the name, address, phone/fax number, e-mail of the Security Officer of the facility to be visited;

f) the purpose of the visit, including the highest security classification level of Classified Information to be involved;

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

h) the date and signature of the sending Competent Security Authority.

(3) In urgent cases, the Competent Security Authorities can agree on a shorter period for the submission of the request for visit.

(4) The Competent Security Authorities may agree on a list of visitors entitled to recurring visits. The list shall be valid for an initial period not exceeding 12 months and may be extended for a further period of time not exceeding 12 months. A request for recurring visits shall be submitted in accordance with Paragraph 2 of this Article. Once the list has been approved, visits may be arranged directly between the facilities involved.

(5) Each Party shall guarantee the protection of personal data of the visitors in accordance with the national laws and regulations.

ARTICLE 12

BREACH OF SECURITY

(1) In case of a security breach resulting in unauthorised disclosure, misappropriation or loss of Classified Information or suspicion of such a breach, the Competent Security Authority of the Recipient Party shall immediately inform the Competent Security Authority of the Originating Party thereof in writing.

(2) The competent Party shall undertake all measures in accordance with the national laws and regulations so as to limit the consequences of the breach referred to in Paragraph 1 of this Article and to prevent further breaches. On request, the other Party shall provide appropriate assistance; it shall be informed of the outcome of the proceedings and the measures undertaken due to the breach.

(3) When the breach of security has occurred in a Third Party, the Competent Security Authority of the sending Party shall take the actions referred to in paragraph 2 of this Article without delay.

(4) The Competent Security Authorities shall inform each other of exceptional security risks that may endanger the released Classified Information.

ARTICLE 13

EXPENSES

(1) The implementation of this Agreement does not include any cost.

(2) In case that, in the course of the implementation of this Agreement, there are unexpected costs for any of the Parties, each Party shall bear its own expenses.

ARTICLE 14

SETTLEMENT OF DISPUTES

Any dispute regarding the interpretation or application of this Agreement shall be settled by consultations and negotiations between the Parties. Meanwhile the Parties will continue to fulfil the provisions set forth in this Agreement.

ARTICLE 15

FINAL PROVISIONS

(1) This Agreement shall enter into force on the first day of the second month from the date of receipt of the latest written notification by which the Parties have informed each other,

through diplomatic channels, that their internal legal requirements necessary for its entry into force have been fulfilled.

(2) This Agreement may be amended by mutual written consent of the Parties. Amendments shall enter into force in accordance with Paragraph 1 of this Article.

(3) This Agreement is concluded for an indefinite period of time. Either Party may denounce this Agreement by giving the other Party notice in writing through diplomatic channels. In that case, this Agreement shall terminate six months from the date on which the other Party has received the denunciation notice.

(4) In case of termination of this Agreement, all Classified Information transferred pursuant to this Agreement shall continue to be protected in accordance with the provisions set forth herein and, upon request, returned to the Originating Party.

(5) Implementing arrangements may be concluded for the implementation of this Agreement.

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

Done in Rome on 20 April 2017 in three originals in the Italian, French and English languages, the French and Italian texts being equally authentic. In case of any divergence of interpretation, the English text shall prevail.

On behalf of the Government of the Italian Republic

On behalf of the Government of the Grand Duchy of Luxemburg