

**ACCORDO TRA
IL GOVERNO DELL' UNGHERIA ED IL GOVERNO DELLA
REPUBBLICA ITALIANA
PER LO SCAMBIO E LA RECIPROCA PROTEZIONE
DELLE INFORMAZIONI CLASSIFICATE**

Il Governo dell'Ungheria e il Governo della Repubblica Italiana (qui di seguito denominate "le Parti"),

Riconoscendo l'importante ruolo della loro reciproca cooperazione tra le Parti,

Riconoscendo che una buona cooperazione può richiedere scambio di informazioni classificate tra le Parti,

Riconoscendo l'interesse che le Parti assicurino equivalente protezione alle informazioni classificate,

Desiderando sostituire l'Accordo tra il Governo della Repubblica Italiana e il Governo della Repubblica di Ungheria sulla reciproca protezione delle informazioni classificate firmato il 20 marzo del 2003 con una nuova versione,

In considerazione del reciproco rispetto per gli interessi nazionali e per la sicurezza, hanno concordato quanto segue:

ARTICOLO 1 SCOPO E AMBITI DI APPLICAZIONE DELL'ACCORDO

1. L'obiettivo di questo Accordo è di assicurare la protezione delle informazioni classificate scambiate o generate nel corso delle cooperazione tra le Parti o tra persone giuridiche o fisiche sotto la propria giurisdizione.
2. Questo Accordo non avrà effetto sugli obblighi assunti dalle parti sotto ogni altro trattato bilaterale o multilaterale, in particolare il trattato della NATO, o sulle obbligazioni derivanti dall'appartenenza all'UE ivi incluso ogni Accordo che regola lo scambio e la reciproca protezione delle informazione classificate.

ARTICOLO 2 DEFINIZIONI

Per gli scopi di questo Accordo:

- a) **"Informazione Classificata"** significa ogni informazione, a prescindere dalla sua forma o natura, secondo le leggi ed i regolamenti di ogni Parte, che richiede protezione contro ogni violazione alla sicurezza ed è stata debitamente definita;
- b) **"Violazione della Sicurezza"** significa un'azione o un'omissione contraria a questo Accordo o contrario alle leggi e ai regolamenti delle Parti, che può comportare la divulgazione, perdita, distruzione o appropriazione indebita, accesso non autorizzato o ogni altro tipo di compromissione delle Informazioni Classificate.

- c) **“Parte Originatrice”** significa la Parte, incluse le entità giuridiche e persone sotto la sua giurisdizione, che rilascia l'Informazione Classificata;
- d) **“Parte Ricevente”** significa la Parte, incluse le entità giuridiche e persone sotto la sua giurisdizione, che riceve l'Informazione Classificata;
- e) **“Parte Terza”** significa qualsiasi Stato, incluse le entità giuridiche e persone sotto la sua giurisdizione, od organizzazione internazionale non facente parte di questo Accordo;
- f) **“Necessità di Conoscere”** significa il principio secondo il quale l'accesso a specifiche Informazioni Classificate può essere concesso solo a quelle persone che hanno una effettiva necessità di accedere ad una data Informazione Classificata in considerazione delle rispettive funzioni ufficiali e/o dello svolgimento di un effettivo incarico ufficiale;
- g) **“Certificato di Abilitazione di Sicurezza Personale”** significa la determinazione positiva dell'Autorità di Sicurezza Nazionale con cui si attesta che un individuo è idoneo ad accedere alle informazioni classificate „Bizalmas!”/RISERVATISSIMO/CONFIDENTIAL o superiore, in conformità con le rispettive leggi e regolamenti nazionali;
- h) **“Contratto Classificato”** significa un contratto che implica o richiede l'accesso ad Informazioni Classificate;
- i) **“Contraente”** significa la persona fisica o giuridica in possesso della capacità di agire al fine di concludere contratti classificati in conformità con le rispettive leggi e regolamenti nazionali;
- l) **Certificato di Abilitazione di Sicurezza industriale** significa la determinazione positiva della Autorità di Sicurezza Nazionale con cui si attesta che una persona giuridica, in possesso della capacità di agire, ha la capacità strutturale ed organizzativa per trattare e conservare informazioni classificate „Bizalmas!”/RISERVATISSIMO/CONFIDENTIAL o superiore, in conformità con le rispettive leggi e regolamenti nazionali;
- m) **“Autorità Nazionale per la Sicurezza”** significa l'autorità nazionale competente ad assicurare l'applicazione delle leggi e dei regolamenti nel settore della protezione delle Informazioni Classificate e che è garante dell'attuazione e della supervisione del presente Accordo.

ARTICOLO 3 AUTORITÀ NAZIONALI PER LA SICUREZZA

1) Le Autorità Nazionali per la Sicurezza delle Parti sono:

In Ungheria:
Nemzeti Biztonsági Felügyelet
(Autorità di Sicurezza Nazionale)

Nella Repubblica Italiana:

Dipartimento delle Informazioni per la Sicurezza – Organo Nazionale di Sicurezza

- 2) Le Autorità Nazionali per la Sicurezza si comunicano reciprocamente i punti di contatto ufficiali ed ogni successivo cambiamento.

Articolo 4

Livelli di classifiche di segretezza

L'equivalenza dei livelli di classifica di sicurezza nazionale è il seguente:

In Ungheria	Nella Repubblica Italiana	Equivalente in lingua Inglese
„Szigorúan titkos!”	SEGRETISSIMO	TOP SECRET
„Titkos!”	SEGRETO	SECRET
„Bizalmas!”	RISERVATISSIMO	CONFIDENTIAL
„Korlátozott terjesztésű!”	RISERVATO	RESTRICTED

ARTICOLO 5

ACCESSO ALLE INFORMAZIONI CLASSIFICATE

L'accesso alle Informazioni Classificate all'insegna di quest'Accordo è limitato solo alle persone autorizzate in virtù del principio della Necessità di Conoscere e debitamente abilitate in conformità con le leggi e i regolamenti nazionali delle rispettive Parti.

ARTICOLO 6

PRINCIPI SULLA SICUREZZA

1. La Parte Originatrice deve:

- a) assicurare che l'Informazione Classificata sia contrassegnata con gli adeguati livelli di classifica di segretezza in conformità con le rispettive leggi e regolamenti nazionali;
- b) informare la Parte Ricevente di ogni condizione d'uso delle Informazioni Classificate;
- c) informare la Parte Ricevente in forma scritta e senza ingiustificati ritardi di ogni successivo cambiamento nella classifica di segretezza o nella durata della classifica.

2. La Parte Ricevente deve:

- a) assicurare che l'Informazione Classificata rechi i corrispondenti contrassegni previsti in conformità con l'art. 4 di questo Accordo;
- b) assicurare all'Informazione Classificata un equivalente livello di protezione assicurato alle proprie Informazioni Classificate con lo stesso livello di classifica di segretezza;
- c) assicurare che l'Informazione Classificata non sia declassificata o ne venga cambiato il livello di classifica di segretezza senza la previa autorizzazione scritta della Parte Originatrice.

- d) assicurare che l'Informazione Classificata non sia ceduta a Parti Terze senza il previo consenso scritto della Parte Originatrice
- e) utilizzare l'Informazione Classificata solo per gli scopi per cui è stata rilasciata e solo entro le condizioni di rilascio previste dalla Parte Originatrice.

ARTICOLO 7 COOPERAZIONE DI SICUREZZA

1. Al fine di mantenere un corrispondente livello di standard di sicurezza, le Autorità di Sicurezza Nazionali dovranno, su richiesta, informare l'un l'altra sulle leggi e regolamenti nazionali inerenti la protezione delle Informazioni Classificate e sulle procedure derivanti dalla loro attuazione.
2. Su richiesta, le Autorità di Sicurezza Nazionali coopereranno e si daranno reciproca assistenza sulle procedure di controllo per il rilascio di Certificato di Abilitazione.
3. Le Parti devono, in accordo con le rispettive leggi e regolamenti nazionali, riconoscere i Certificati di Abilitazione Personali ed Industriali rilasciati dall'altra Parte in accordo con l'Art. 4 di questo Accordo.
4. Le Autorità di Sicurezza Nazionali e le altre organizzazioni di sicurezza competenti, in conformità con le rispettive leggi ed i regolamenti nazionali, devono prontamente notificare l'un l'altra le modifiche nei Certificati di Abilitazione Personali ed Industriali, specialmente in caso di ritiro.
5. La cooperazione sotto questo accordo viene attuata in lingua inglese.

ARTICOLO 8 CONTRATTI CLASSIFICATI

1. I Contratti Classificati devono essere conclusi ed eseguiti in conformità con le legislazioni nazionali delle Parti. Su richiesta, l'Autorità Nazionale di Sicurezza di ciascuna Parte deve assicurare che ad un proposto Contraente così come le persone che partecipano alle negoziazioni precontrattuali o all'esecuzione dei contratti con un livello di classifica „Bizalmas!”/RISERVATISSIMO/CONFIDENTIAL o superiore, sia stata rilasciata la prevista Abilitazione di Sicurezza Personale o Industriale.
2. L'Autorità Nazionale di Sicurezza può richiedere alla controparte informazioni di sicurezza relative all'installazione sita nel territorio dell'altra parte al fine di assicurare la costante protezione delle Informazioni Classificate.
3. I Contratti con un livello di classifica „Bizalmas!”/RISERVATISSIMO/CONFIDENTIAL o superiore devono contenere, come parte integrante del contratto, istruzioni sulla sicurezza del progetto e sul livello di classifica di segretezza di ogni elemento del contratto Classificato. Una copia della clausola di sicurezza viene trasmessa all'Autorità Nazionale di Sicurezza della Parte sotto la cui giurisdizione il Contratto verrà eseguito.

4. I contratti con un livello di classifica „Korlátozott terjesztésű!”/RISERVATO/RESTRICTED devono contenere una specifica clausola di sicurezza che identifica le misure di sicurezza minime che devono essere applicate per la protezione delle Informazioni Classificate.

ARTICOLO 9

TRASFERIMENTO O TRASMISSIONE DELLE INFORMAZIONI CLASSIFICATE

1. Le Informazioni Classificate saranno trasferite in accordo con le leggi e i regolamenti nazionali della Parte Originatrice attraverso canali diplomatici o come concordato in forma scritta tra le Autorità Nazionali di Sicurezza.
2. Le Parti possono trasmettere Informazioni Classificate tramite sistemi elettronici in accordo con le procedure di sicurezza approvate in forma scritta dalle Autorità Nazionali di Sicurezza.

ARTICOLO 10

RIPRODUZIONE E TRADUZIONE DELLE INFORMAZIONI CLASSIFICATE

1. Le riproduzioni e le traduzioni delle Informazioni Classificate rilasciate sotto questo Accordo devono essere contrassegnate con l'appropriato livello di classifica e protette come gli originali. Il numero di riproduzioni sarà limitato a quanto richiesto dagli scopi ufficiali.
2. Le traduzioni delle Informazioni Classificate rilasciate in virtù di questo Accordo devono recare una nota nella lingua nella quale è stata tradotta che specifichi che la traduzione contiene Informazioni Classificate della Parte Originatrice.
3. Le Informazioni Classificate rilasciate in virtù di questo Accordo di livello „Szigorúan titkos!”/SEGRETISSIMO/TOP SECRET devono essere tradotte o riprodotte solo previo il consenso scritto della Parte Originatrice.
4. Le Informazioni Classificate rilasciate in virtù di questo Accordo con un livello di classifica „Szigorúan titkos!”/SEGRETISSIMO/TOP SECRET non devono essere distrutte e devono essere riconsegnate alla Parte Originatrice.
5. In caso di emergenza l'Informazione Classificata, che risulta impossibile proteggere o riconsegnare alla Parte Originatrice, deve essere distrutta senza ingiustificati ritardi. L'Autorità Nazionale di Sicurezza della Parte Ricevente deve notificare in forma scritta alla Parte Originatrice la distruzione dell'Informazione Classificata.

Articolo 11

Visite

1. Le visite che richiedono accesso a Informazioni Classificate sono sottoposte alla preventiva autorizzazione in forma scritta dell'Autorità Nazionale di Sicurezza delle rispettive Parti.
2. L'Autorità Nazionale di Sicurezza della Parte che effettua la visita notifica all'Autorità Nazionale di Sicurezza della Parte ospitante circa la visita pianificata attraverso una richiesta di visita trasmessa almeno venti giorni prima rispetto alla data pianificata. Nei casi urgenti, la richiesta di visita potrà essere sottoposta a più breve distanza, soggetta ad un preventivo coordinamento tra le Autorità Nazionali di Sicurezza.
3. La richiesta di visita deve comprendere:
 - a) il nome del visitatore, la data e il luogo di nascita, la nazionalità e il numero del passaporto/CI;
 - b) la posizione del visitatore e il nome dell'organizzazione rappresentata;
 - c) il livello di Abilitazione di Sicurezza Personale del visitatore e la sua validità;
 - d) data e durata della visita e, nel caso di visite ricorrenti, il periodo totale delle visite;
 - e) scopo della visita e livello massimo di classifica dell'Informazione Classificata;
 - f) nome ed indirizzo delle organizzazioni ed infrastrutture da visitare e l'indicazione del punto di contatto, comprensivo del nome e cognome, indirizzo di posta elettronica e numero telefonico/FAX;
 - g) data, firma e contrassegno ufficiale dell'Autorità Nazionale di Sicurezza.
4. Le Autorità Nazionali di Sicurezza possono accordarsi su una lista di visitatori autorizzati ad effettuare visite ricorrenti. In caso di contratti o progetti classificati che richiedono visite ricorrenti, le Autorità Nazionali di Sicurezza delle Parti comunicano tra loro inviando l'un l'altro una lista di personale autorizzato in conformità con le leggi ed i regolamenti nazionali. Tale lista non può essere valida per un periodo superiore a dodici mesi. Una volta che la lista è stata approvata, le visite potranno essere concordate direttamente in conformità alle leggi ed i regolamenti nazionali.
5. Le Informazioni Classificate acquisite da un visitatore sono considerate Informazioni Classificate ricevute in virtù di questo Accordo.

ARTICOLO 12

VIOLAZIONI ALLA SICUREZZA

1. Le Autorità Nazionali di Sicurezza si informano senza ingiustificato ritardo ed in forma scritta di ogni violazione alla sicurezza od in caso di grave sospetto.

2. L'Autorità Nazionale di Sicurezza della Parte dove la Violazione alla Sicurezza è occorsa, senza indebito ritardo, indaga o avvia indagini sull'incidente. L'Autorità Nazionale di Sicurezza dell'altra Parte, ove richiesto, coopera nelle indagini.
3. In ogni caso, l'Autorità Nazionale di Sicurezza della Parte Ricevente informa l'Autorità Nazionale di Sicurezza della Parte Originatrice in forma scritta delle circostanze della Violazione alla Sicurezza, della portata del danno, delle misure adottate per il suo contenimento e le risultanze delle indagini
4. Quando la Violazione alla Sicurezza è avvenuta presso una Parte Terza, l'Autorità Nazionale per la Sicurezza che ha rilasciato l'Informazione Classificata alla Parte Terza deve adottare tutte le possibili azioni per assicurare che le misure previste in quest'articolo vengano applicate.

ARTICOLO 13 COSTI

L'attuazione di questo Accordo non prevede alcuna spesa. Qualora dovessero verificarsi dei costi, ognuna delle Parti sosterrà i propri.

ARTICOLO 14 DISPOSIZIONI FINALI

1. Questo Accordo rimane in vigore per un periodo di tempo indeterminato. Questo Accordo entra in vigore dal primo giorno del secondo mese successivo alla data di ricezione dell'ultima notifica tra le Parti, attraverso canali diplomatici, e afferma che le procedure per l'entrata in vigore di questo Accordo sono state ottemperate.
2. Questo Accordo può essere emendato attraverso il reciproco consenso scritto tra le Parti. Gli emendamenti entrano in vigore in conformità con le disposizioni del paragrafo 1 di questo Articolo.
3. Ciascuna delle Parti può denunciare in qualsiasi momento questo Accordo informando l'altra per iscritto. In tal caso, questo Accordo termina sei (6) mesi dopo la data con la quale l'altra Parte ha ricevuto la notizia di denuncia.
4. A prescindere dalla caducazione di questo Accordo, tutte le Informazioni Classificate scambiate o generate all'insegna di questo Accordo saranno protette secondo le previsioni stabilite accluse, finché la Parte Originatrice dispensa la Parte Ricevente da questo obbligo in forma scritta.
5. Qualsiasi disputa relativa all'interpretazione o l'attuazione di questo Accordo sarà risolta attraverso consultazione e negoziazioni tra le Parti, senza il ricorso all'Autorità Giudiziaria.
6. Con l'entrata in vigore di questo Accordo, l'Accordo tra il Governo della Repubblica di Ungheria e il Governo della Repubblica Italiana e sulla reciproca protezione delle Informazioni Classificate firmato il 20 marzo del 2003 termina la sua validità.

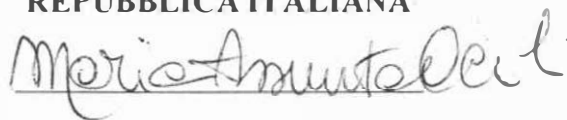
In fede, i sottoscritti Rappresentanti, debitamente autorizzati dai rispettivi Governi, firmano il presente Accordo.

Fatto a Budapest il 26 novembre 2015 in due originali, in lingua Ungherese, Italiana ed Inglese, essendo entrambi i testi egualmente autentici. In caso di divergenze di interpretazione, prevale il testo Inglese.

PER IL GOVERNO DELL'UNGHERIA

A handwritten signature in black ink, consisting of a large loop followed by a horizontal line and a small flourish, positioned above a solid horizontal line.

**PER IL GOVERNO DELLA
REPUBBLICA ITALIANA**

A handwritten signature in black ink, written in a cursive style, positioned above a solid horizontal line.

EGYEZMÉNY

Magyarország Kormánya és az Olasz Köztársaság Kormánya között a minősített adatok cseréjéről és kölcsönös védelméről

Magyarország Kormánya és az Olasz Köztársaság Kormánya, a továbbiakban együtt: „Felek”,
Elismerve a Felek közötti kölcsönös együttműködés jelentőségét,

Felismerve, hogy a Felek közötti együttműködés során szükség lehet minősített adatok
cseréjére,

Elismerve az azonos szintű védelem biztosításának igényét a minősített adatok számára,

Új egyezményrel kívánva kiváltani a Magyar Köztársaság Kormánya és az Olasz Köztársaság
Kormánya között a minősített információk kölcsönös védelméről szóló, 2003. március 20-án
aláírt Biztonsági Megállapodást,

Kölcsönösen tiszteletben tartva egymás nemzeti érdekeit és biztonságát, az alábbiakban
állapodtak meg:

1. Cikk

Az Egyezmény célja és alkalmazási területe

1. Jelen Egyezmény célja, hogy védelmet biztosítson a Felek, valamint a joghatóságuk alá
tartozó jogi személyek és természetes személyek közötti együttműködés keretében kicserélt
vagy keletkezett minősített adatok számára.

2. Jelen Egyezmény nem érinti a Felek egyéb két-, vagy többoldalú szerződés, különösen
NATO szerződés alapján fennálló vagy Európai Unió tagságból eredő kötelezettségeit,
ideértve mindazon megállapodásokat is, amelyek minősített adatok cseréjét és kölcsönös
védelmét szabályozzák.

2. Cikk

Fogalommeghatározások

Jelen Egyezmény alkalmazásában:

a) A „**Minősített Adat**” megjelenési formájától vagy természetétől függetlenül, minden olyan
adat, amelyet bármelyik Fél nemzeti jogszabályai vagy egyéb szabályai szerint védelemben
kell részesíteni a minősített adat biztonságának megsértésével szemben, s amelyet ennek
megfelelően minősítettek;

b) A „**Minősített adat biztonságának megsértése**” olyan, a jelen Egyezménnyel és a Felek
saját nemzeti jogszabályaival vagy egyéb szabályaival ellentétes tevékenységet vagy
mulasztást jelent, melynek következtében a minősített adat jogosulatlan nyilvánosságra
hozatala, elvesztése, megsemmisülése, jogosulatlan felhasználása, megszerzése vagy egyéb
módon történő megsértése következhet be;

c) Az „**Átadó Fél**” azt a Felet, valamint a joghatósága alá tartozó jogi személyeket vagy
természetes személyeket jelenti, amelyik a minősített adatot átadja;

d) Az „**Átvevő Fél**” azt a Felet, valamint a joghatósága alá tartozó jogi személyeket vagy
természetes személyeket jelenti, amelyik a minősített adatot átveszi;

e) A **„Harmadik Fél”** bármely olyan államot, valamint a joghatósága alá tartozó jogi személyeket vagy természetes személyeket, továbbá nemzetközi szervezetet jelent, amely nem részese jelen Egyezménynek;

f) A **„Szükséges Ismeret”** azt a követelményt jelenti, amely alapján egy meghatározott minősített adathoz való hozzáférés csak annak a személynek biztosítható, akinek a hozzáférés hivatali kötelessége vagy meghatározott feladata ellátásához igazoltan szükséges;

g) A **„Személyi Biztonsági Tanúsítvány”** a Nemzeti Biztonsági Felügyelet azon döntése, amely szerint a természetes személy a nemzeti jogszabályok és egyéb szabályok rendelkezéseinek tiszteletben tartásával hozzáférhet **„Bizalmas!”/ RISERVATISSIMO/ CONFIDENTIAL** vagy magasabb szintű minősített adatokhoz;

h) A **„Minősített szerződés”** olyan szerződést jelent, amely minősített adatot tartalmaz vagy amely alapján minősített adathoz történő hozzáférés szükséges;

i) A **„Szerződő”** olyan természetes személy vagy jogi személy, amely a nemzeti jogszabályok vagy egyéb szabályok rendelkezéseivel összhangban jogképességgel rendelkezik minősített szerződések megkötésére;

j) A **„Telephely Biztonsági Tanúsítvány”** a Nemzeti Biztonsági Felügyelet azon döntése, amely szerint a jogképességgel rendelkező jogi személy vagy természetes személy rendelkezik azon fizikai és szervezeti képességekkel, amely alkalmassá teszik a **„Bizalmas!”/ RISERVATISSIMO/ CONFIDENTIAL** vagy magasabb szintű minősített adatok kezelésére és tárolására a nemzeti jogszabályok és egyéb szabályok rendelkezéseinek megfelelően;

k) A **„Nemzeti Biztonsági Felügyelet”** az a nemzeti hatóság, amely a minősített adatok védelme vonatkozásában felelős a nemzeti jogszabályok és egyéb szabályok rendelkezéseinek pontos betartásáért, valamint jelen Egyezmény alkalmazásáért és felügyeletéért.

3. Cikk

Nemzeti Biztonsági Felügyelet

1. A Felek Nemzeti Biztonsági Felügyeletei a következők:

Magyarországon:

Nemzeti Biztonsági Felügyelet

Az Olasz Köztársaságban:

Információbiztonsági Osztály-Nemzeti Biztonsági Testület (Dipartimento delle Informazioni per la Sicurezza – Organo Nazionale di Sicurezza)

2. A Nemzeti Biztonsági Felügyelet kötelesek tájékoztatni egymást hivatalos elérhetőségi adataikról, valamint az ezzel kapcsolatos változásokról.

4. Cikk

Minősítési szintek megfeleltetése

Az egyes nemzeti minősítési szintek az alábbiak szerint feleltethetők meg egymásnak:

Magyarországon	Az Olasz Köztársaságban	Angol nyelvű megfelelőjük
„Szigorúan titkos!”	SEGRETISSIMO	TOP SECRET
„Titkos!”	SEGRETO	SECRET
„Bizalmas!”	RISERVATISSIMO	CONFIDENTIAL
„Korlátozott terjesztésű!”	RISERVATO	RESTRICTED

5. Cikk

Minősített adathoz való hozzáférés

Minősített adathoz jelen Egyezmény alapján kizárólag olyan természetes személyek jogosultak hozzáférni, akik a Szükséges Ismeret elvének megfelelnek és az érintett Fél nemzeti jogszabályaival és egyéb szabályaival összhangban erre megfelelő felhatalmazást kaptak.

6. Cikk

Biztonsági alapelvek

1. Az Átadó Fél:

- a) köteles biztosítani, hogy a minősített adaton a nemzeti jogszabályai és egyéb szabályai szerinti megfelelő minősítési szint feltüntetésre kerüljön;
- b) köteles tájékoztatni az Átvevő Felet a minősített adat felhasználásának esetleges feltételhez kötéséről;
- c) haladéktalanul köteles írásban tájékoztatni az Átvevő Felet az adat minősítési szintjében bekövetkezett változásokról.

2. Az Átvevő Fél:

- a) köteles biztosítani, hogy a minősített adaton feltüntetésre kerüljön jelen Egyezmény 4. Cikke alapján meghatározott egyenértékű minősítési szint;
- b) ugyanolyan szintű védelemben köteles részesíteni a másik Félről kapott minősített adatot, mint amelyet a saját, azonos minősítési szintű minősített adata számára biztosít;
- c) köteles biztosítani, hogy az Átadó Fél előzetes írásbeli hozzájárulása nélkül a minősített adat minősítését nem szüntetik meg, illetve minősítési szintjét nem változtatják meg;
- d) köteles biztosítani, hogy az Átadó Fél előzetes írásbeli hozzájárulása nélkül az átvett minősített adatot Harmadik Fél részére nem adja át;
- e) a minősített adatot kizárólag az átadás során megjelölt célra használhatja fel, betartva az Átadó Fél által meghatározott feltételeket.

7. Cikk

Biztonsági együttműködés

1. A hasonló szintű biztonsági követelmények fenntartása érdekében a Nemzeti Biztonsági Felügyelet megkeresésre kötelesek egymást tájékoztatni a minősített adat védelmével kapcsolatos nemzeti jogszabályokról és egyéb szabályokról, valamint mindezek gyakorlati alkalmazásáról.

2. Megkeresés esetén a Nemzeti Biztonsági Felügyelet, kötelesek egymással együttműködni és egymásnak segítséget nyújtani a személyi biztonsági tanúsítványok kiállításával kapcsolatos biztonsági ellenőrzések során.

3. A Felek kötelesek nemzeti jogszabályaik és egyéb szabályaik rendelkezéseivel összhangban elismerni a másik Fél által, jelen Egyezmény 4. Cikkében foglaltaknak megfelelően kibocsátott személyi biztonsági tanúsítványokat és telephely biztonsági tanúsítványokat.

4. A Nemzeti Biztonsági Felügyelet vagy más, hatáskörrel rendelkező biztonsági szervezetek kötelesek nemzeti jogszabályaik és egyéb szabályaik rendelkezéseivel összhangban, haladéktalanul értesíteni egymást az elismert személyi biztonsági tanúsítványokkal és a telephely biztonsági tanúsítványokkal kapcsolatos változásokról, különösen azok visszavonásáról.

5. Jelen Egyezmény során megvalósuló együttműködés angol nyelven történik.

8. Cikk

Minősített szerződések

1. A minősített szerződéseket a Felek saját nemzeti jogszabályai és egyéb szabályai alapján kell megkötöni és teljesíteni. A Nemzeti Biztonsági Felügyelet megkeresésre kötelesek megerősíteni, hogy az ajánlattevők és a szerződéskötést megelőző tárgyalásokban vagy a „Bizalmas!”/ RISERVATISSIMO/ CONFIDENTIAL vagy magasabb minősítési szintre minősített szerződések teljesítésében részt vevő természetes személyek rendelkeznek megfelelő személyi biztonsági tanúsítvánnyal vagy telephely biztonsági tanúsítvánnyal.

2. A Nemzeti Biztonsági Felügyelet információt kérhet a másik Fél Nemzeti Biztonsági Felügyeletétől a másik Fél területén lévő létesítményre vonatkozó biztonsági helyzettel kapcsolatban a minősített adat folyamatos védelmének biztosítása céljából.

3. A „Bizalmas!”/ RISERVATISSIMO/ CONFIDENTIAL vagy magasabb minősítési szintre minősített szerződések lényeges részét képezi a projekt biztonsági utasítás, amely a biztonsági követelményeket és a minősített szerződés egyes elemeinek minősítésével kapcsolatos rendelkezéseket határozza meg. A projekt biztonsági utasítás másolatát azon Fél Nemzeti Biztonsági Felügyelete részére kell továbbítani, amelynek joghatósága alatt a minősített szerződés végrehajtása történik.

4. A „Korlátozott terjesztésű!”/ RISERVATO/ RESTRICTED minősítésű minősített szerződés biztonsági záradékot tartalmaz, amely a minősített adat védelmét biztosító minimum biztonsági intézkedéseket határozza meg.

9. Cikk

A minősített adat továbbítása

1. A minősített adat továbbítása az Átadó Fél nemzeti jogszabályaiban és egyéb szabályaiban meghatározott szabályok szerint, diplomáciai úton, vagy a Nemzeti Biztonsági Felügyelet által írásban meghatározott egyéb módon történik.

2. A Felek, a Nemzeti Biztonsági Felügyelet által írásban jóváhagyott eljárási rend szerint, elektronikus úton is továbbíthatnak minősített adatot.

10. Cikk

A minősített adat sokszorosítása, fordítása és megsemmisítése

1. Jelen Egyezmény alapján átadott minősített adatról készült másolatokon és fordításokon fel kell tüntetni a megfelelő minősítési jelölést és az így készült adatot ugyanolyan védelemben kell részesíteni, mint az eredeti minősített adatot. A sokszorosított példányok számát a hivatalos célból szükséges mértékre kell korlátozni.
2. Jelen Egyezmény alapján átadott minősített adat fordítása során keletkező példányokon a fordítás nyelvén fel kell tüntetni, hogy az az Átadó Fél minősített adatát tartalmazza.
3. Jelen Egyezmény alapján átadott, „Szigorúan titkos!”/ SECRETISSIMO/ TOP SECRET minősítésű adat fordítása vagy sokszorosítása kizárólag az Átadó Fél előzetes írásbeli engedélyével lehetséges.
4. Jelen Egyezmény alapján átadott, „Szigorúan titkos!”/ SECRETISSIMO/ TOP SECRET minősítésű adat nem semmisíthető meg, az ezen minősítési szintű adatokat az Átadó Félnek kell visszaszolgáltatni.
5. Olyan válsághelyzet esetén, amely lehetetlenné teszi a minősített adat védelmét, vagy az Átadó Félnek való visszajuttatását, a minősített adatot haladéktalanul meg kell semmisíteni. Az Átvevő Fél Nemzeti Biztonsági Felügyelete köteles az Átadó Fél Nemzeti Biztonsági Felügyeletét írásban értesíteni a minősített adatok megsemmisítéséről.

11. Cikk Látogatások

1. Minősített adathoz való hozzáférést igénylő látogatásra az érintett Nemzeti Biztonsági Felügyelet előzetes írásbeli jóváhagyása alapján kerülhet sor.
2. A látogató Fél Nemzeti Biztonsági Felügyelete köteles a fogadó Fél Nemzeti Biztonsági Felügyeletét látogatásra vonatkozó megkeresésében legalább húsz nappal a látogatás időpontja előtt tájékoztatni a tervezett látogatásról. Sürgős esetben, a Nemzeti Biztonsági Felügyelet előzetes egyeztetését követően a látogatásra vonatkozó megkeresés a látogatás kezdetéhez közelebbi időpontban is benyújtható.
3. A látogatásra vonatkozó megkeresésnek az alábbiakat kell tartalmaznia:
 - a) a látogató neve, születési helye és ideje, állampolgársága, útlevelének vagy más személyazonosító igazolványának száma;
 - b) a látogató beosztásának és a látogató által képviselt jogi személynek a megjelölése;
 - c) a látogató személyi biztonsági tanúsítványának szintje és érvényességi ideje;
 - d) a látogatás időpontja és időtartama, visszatérő látogatások esetén az egyes látogatások összesített időtartama;
 - e) a látogatás célja, valamint a megismerendő legmagasabb minősítési szintű minősített adat minősítési szintjének megjelölése;
 - f) a meglátogatandó létesítmény neve és címe, valamint a kapcsolattartójának neve, telefonszáma, faxszáma, e-mail címe;
 - g) dátum, aláírás és a Nemzeti Biztonsági Felügyelet hivatalos pecsétjének lenyomata.
4. A Nemzeti Biztonsági Felügyelet közösen meghatározhatja a visszatérő látogatásra jogosult személyek listáját. Azon projektek vagy szerződések esetén, amelyben szükséges a látogatás megisméltése a Felek Nemzeti Biztonsági Felügyeletei kötelesek egymást tájékoztatni a felhatalmazott személyek listájának megküldésével nemzeti jogszabályaik és egyéb szabályaik rendelkezéseivel összhangban. A lista érvényessége nem lehet hosszabb, mint tizenkét hónap. Amennyiben a lista elfogadásra kerül, a látogatások a nemzeti jogszabályok és egyéb szabályok rendelkezéseivel összhangban közvetlenül lefolytathatók.
5. A látogató által megismert minősített adatot úgy kell tekinteni, mint a jelen Egyezmény alapján átvett minősített adatot.

12. Cikk

Eljárás a minősített adat biztonságának megsértése esetén

1. A Nemzeti Biztonsági Felügyeletek késedelem nélkül írásban tájékoztatják egymást a minősített adat biztonságának megsértéséről vagy ennek alapos gyanújáról.
2. Azon Fél Nemzeti Biztonsági Felügyelete, ahol a minősített adat biztonságának megsértésére sor került, késedelem nélkül intézkedik a minősített adat megsértésének kivizsgálása érdekében. A másik Fél Nemzeti Biztonsági Felügyelete szükség esetén részt vesz a vizsgálatban.
3. Az Átvevő Fél Nemzeti Biztonsági Felügyelete minden esetben írásban tájékoztatja az Átadó Fél Nemzeti Biztonsági Felügyeletét a minősített adat biztonsága megsértésének körülményeiről, a kár mértékéről, a kár enyhítése érdekében megtett intézkedésekről, valamint a vizsgálat eredményéről.
4. Ha a minősített adat biztonságának megsértése harmadik Félnél következik be, az a Nemzeti Biztonsági Felügyelet, amely a minősített adatot a harmadik Félnak átadta köteles megtenni minden lehetséges intézkedést jelen Cikkben meghatározott előírások megvalósulásának biztosítása érdekében.

13. Cikk

Költségek viselése

Jelen Egyezmény végrehajtása nem jár költségekkel. Az esetlegesen mégis felmerülő költségeket a Felek maguk viselik.

14. Cikk

Záró rendelkezések

1. Jelen Egyezmény határozatlan időre jön létre. Jelen Egyezmény a Felek az Egyezmény hatálybalépéshez szükséges belső feltételek teljesítésére vonatkozó, diplomáciai úton küldött utolsó értesítése kézhezvételének napját követő második hónap első napján lép hatályba.
 2. Jelen Egyezmény a Felek kölcsönös egyetértésével írásban módosítható. A módosítások hatályba lépésével kapcsolatban a jelen Cikk 1. pontjában foglaltak az irányadók.
 3. Bármelyik Fél jogosult jelen Egyezményt bármikor írásban felmondani. Felmondás esetén az Egyezmény a felmondásról szóló írásbeli értesítés másik Fél általi kézhezvételétől számított 6 hónap elteltével hatályát veszti.
 4. Az Egyezmény megszűnésétől függetlenül az annak alapján átadott vagy keletkeztetett minősített adatokat az Egyezményben meghatározott rendelkezések szerint kell védelemben részesíteni, mindaddig, amíg az Átadó Fél írásban felmentést nem ad az Átvevő Fél részére ezen kötelezettség alól.
 5. Felek a jelen Egyezmény értelmezéséből vagy végrehajtásából fakadó vitákat tárgyalás és egyeztetés útján, külső igazságszolgáltatási fórum igénybe vétele nélkül rendezik.
 6. Jelen Egyezmény hatályba lépésével a Magyar Köztársaság Kormánya és az Olasz Köztársaság Kormánya között a minősített információk kölcsönös védelméről szóló 2003. március 20-án aláírt Biztonsági Megállapodás hatályát veszti.
- Fentiek tanúbizonyságául, az alulírott és az erre felhatalmazott megbízottak jelen Egyezményt aláírásukkal látták el.

Készült Budapesten, 2015. november 26-án, két eredeti példányban, magyar, olasz és angol nyelven, valamennyi szöveg egyaránt hiteles. Eltérés esetén az angol nyelvű szöveg az irányadó.


Magyarország Kormánya
részéről

Az Olasz Köztársaság Kormánya
részéről


Maria Amato

AGREEMENT

Between the Government of Hungary and the Government of the Italian Republic on the Exchange and Mutual Protection of Classified Information

The Government of Hungary and the Government of the Italian Republic, hereinafter referred to as the "Parties",

Recognising the importance of mutual cooperation between the Parties,

Realising that good cooperation may require exchange of Classified Information between the Parties,

Recognising the interest that the Parties ensure equivalent protection for the Classified Information,

Wishing to replace the Agreement between the Government of the Italian Republic and the Government of the Republic of Hungary on the mutual protection of Classified Information signed on 20th March 2003 with a new Agreement,

Have, in mutual respect for national interests and security, agreed upon the following:

ARTICLE 1

OBJECTIVE AND APPLICABILITY OF THE AGREEMENT

1. The objective of this Agreement is to ensure the protection of Classified Information exchanged or generated in the framework of the cooperation between the Parties or between the legal entities or individuals under their jurisdiction.

2. This Agreement shall not affect the obligations of the Parties under any other bilateral or multilateral treaty, in particular NATO treaty, or obligations stemming from EU membership, including any agreements governing exchange and mutual protection of Classified Information.

ARTICLE 2

DEFINITIONS

For the purpose of this Agreement:

a) **"Classified Information"** means any information that, regardless of its form or nature, under the national laws and regulations of either Party, requires protection against breach of security and has been duly designated;

b) **"Breach of Security"** means an act or an omission which is contrary to this Agreement or to the national laws and regulations of the respective Parties, the result of which may lead to unauthorised disclosure, loss, destruction, access, misappropriation or any other type of compromise of Classified Information;

c) **"Originating Party"** means the Party including the legal entities or individuals under its jurisdiction, which releases Classified Information;

d) **"Recipient Party"** means the Party including the legal entities or individuals under its jurisdiction, which receives Classified Information;

e) **"Third Party"** means any State including the legal entities or individuals under its jurisdiction or international organisation not being a party to this Agreement;

f) **"Need-to-know"** means the principle, according to which access to specific Classified Information may only be granted to a person who has a verified need to access this Classified Information in connection with his/her official duties or for the performance of a

specific task;

g) **"Personnel Security Clearance Certificate"** means the determination by the National Security Authority confirming that an individual is eligible to have access to information classified "Bizalmas!" / RISERVATISSIMO / CONFIDENTIAL or above, in accordance with the national laws and regulations;

h) **"Classified Contract"** means a contract that involves or requires access to Classified Information;

i) **"Contractor"** means an individual or a legal entity possessing the legal capacity to conclude Classified Contracts in accordance with the national laws and regulations;

j) **"Facility Security Clearance Certificate"** means the determination by the National Security Authority confirming that a legal entity or an individual possessing the legal capacity, has the physical and organizational capability to handle and store information classified "Bizalmas!" / RISERVATISSIMO / CONFIDENTIAL or above in accordance with the national laws and regulations;

k) **"National Security Authority"** means the national authority competent to ensure the correct implementation of the national laws and regulations in the field of protection of Classified Information and which is responsible for the application and supervision of this Agreement.

ARTICLE 3 NATIONAL SECURITY AUTHORITIES

1. The National Security Authorities of the Parties are:

In Hungary:

Nemzeti Biztonsági Felügyelet
(National Security Authority)

In the Italian Republic:

Dipartimento delle Informazioni per la Sicurezza – Organo Nazionale di Sicurezza
(Department of Information for Security – National Security Body)

2. The National Security Authorities shall provide each other with official contact details and shall inform each other of any subsequent changes thereof.

ARTICLE 4 SECURITY CLASSIFICATION LEVELS AND MARKINGS

The equivalence of national security classification levels and markings is as follows:

In Hungary	In the Italian Republic	Equivalent in English language
„Szigorúan titkos!”	SEGRETISSIMO	TOP SECRET
„Titkos!”	SEGRETO	SECRET
„Bizalmas!”	RISERVATISSIMO	CONFIDENTIAL

„Korlátozott terjesztésű!”	RISERVATO	RESTRICTED
----------------------------	-----------	------------

ARTICLE 5 ACCESS TO CLASSIFIED INFORMATION

Access to Classified Information under this Agreement shall be limited only to individuals upon the Need-to-know principle and who are duly authorized in accordance with the national laws and regulations of the respective Party.

ARTICLE 6 SECURITY PRINCIPLES

1. The Originating Party shall:

- a) ensure that Classified Information is marked with appropriate security classification markings in accordance with its national laws and regulations;
- b) inform the Recipient Party of any use conditions of Classified Information;
- c) inform the Recipient Party in writing without undue delay of any subsequent changes in the security classification level.

2. The Recipient Party shall:

- a) ensure that Classified Information is marked with equivalent security classification marking in accordance with Article 4 of this Agreement;
- b) afford Classified Information received from the other Party a level of security protection that is afforded to its own Classified Information of an equivalent classification level;
- c) ensure that Classified Information is not declassified nor its security classification level changed without the prior written consent of the Originating Party;
- d) ensure that Classified Information is not released to a Third Party without the prior written consent of the Originating Party;
- e) use Classified Information only for the purpose it has been released for and in accordance with release conditions of the Originating Party.

ARTICLE 7 SECURITY COOPERATION

1. In order to maintain comparable standards of security, the National Security Authorities shall, on request, inform each other of their national laws and regulations concerning protection of Classified Information and the practices deriving from their implementation.

2. On request, the National Security Authorities, shall cooperate and give mutual assistance during the vetting procedures for the release of Personnel Security Clearances.

3. The Parties shall, in accordance with their national laws and regulations, recognise the personnel security clearance certificates and facility security clearance certificates issued by the other Party accordingly to Article 4 of this Agreement.

4. The National Security Authorities or other competent security organizations in accordance with national laws and regulations shall promptly notify each other about changes in the recognised personnel security clearance certificates and facility security clearance certificates, especially in case of their withdrawal.

5. The cooperation under this Agreement shall be effected in the English language.

ARTICLE 8 CLASSIFIED CONTRACTS

1. Classified contracts shall be concluded and implemented in accordance with the national laws and regulations of each Party. On request, the National Security Authorities shall confirm that proposed contractors as well as individuals participating in pre-contractual negotiations or in the implementation of contracts classified "Bizalmas!" / RISERVATISSIMO / CONFIDENTIAL and above have appropriate personnel Security Clearance Certificate or Facility Security Clearance Certificate.

2. The National Security Authority may request its counterpart information regarding security situation concerning a facility located in the territory of the other Party to ensure continuing protection of Classified Information.

3. Contracts classified "Bizalmas!" / RISERVATISSIMO / CONFIDENTIAL and above shall contain, as integral part of the contract, project security instructions on the security requirements and on the security classification level of each element of the Classified Contract. A copy of the project security instructions shall be forwarded to the National Security Authority of the Party under whose jurisdiction the Classified Contract is to be implemented.

4. Contracts classified "Korlátozott terjesztésű!" / RISERVATO / RESTRICTED shall contain an appropriate security clause identifying the minimum security measures to be applied for the protection of Classified Information.

ARTICLE 9 TRANSMISSION OF CLASSIFIED INFORMATION

1. Classified Information shall be transmitted in accordance with the national laws and regulations of the Originating Party through diplomatic channels or as otherwise agreed in writing between the National Security Authorities.

2. The Parties may transmit Classified Information by electronic means in accordance with the security procedures approved by the National Security Authorities in writing.

ARTICLE 10 REPRODUCTION, TRANSLATION AND DESTRUCTION OF CLASSIFIED INFORMATION

1. Reproductions and translations of Classified Information released under this Agreement shall bear appropriate security classification markings and shall be protected as the originals. Number of reproductions shall be limited to that required for official purposes.

2. Translations of Classified Information released under this Agreement shall bear a note in the language of translation indicating that they contain Classified Information of the Originating Party.

3. Classified Information released under this Agreement marked „Szigorúan titkos!”/ SEGRETISSIMO/ TOP SECRET shall be translated or reproduced only upon the prior written consent of the Originating Party.

4. Classified Information released under this Agreement marked „Szigorúan titkos!”/ SEGRETISSIMO/ TOP SECRET shall not be destroyed and shall be returned to the Originating Party.

5. In case of a crisis situation in which it is impossible to protect or to return the Classified Information to the Originating Party it shall be destroyed without undue delay. The National Security Authority of the Recipient Party shall notify the National Security Authority of the Originating Party in writing about the destruction of the Classified Information.

ARTICLE 11

VISITS

1. Visits requiring access to Classified Information shall be subject to the prior written consent of the National Security Authority of the respective Party.

2. The National Security Authority of the visiting Party shall notify the National Security Authority of the host Party about the planned visit through a request for visit at least twenty days before the visit takes place. In urgent cases, the request for visit may be submitted at a shorter notice, subject to prior co-ordination between the National Security Authorities.

3. The request for visit shall contain:

- a) visitor's name, date and place of birth, nationality and passport/ID card number;
- b) position of the visitor and specification of the legal entity represented;
- c) visitor's personnel security clearance certificate level and its validity;
- d) date and duration of the visit, and in case of recurring visits the total period of time covered by the visits;
- e) purpose of the visit including the highest security classification level of Classified Information involved;
- f) name and address of the facility to be visited, as well as the name, phone/fax number, e-mail address of its point of contact;
- g) date, signature and stamping of the official seal of the National Security Authority.

4. The National Security Authorities may agree on a list of visitors entitled to recurring visits. In case of projects or contracts which require recurring visits, the National Security Authorities of the Parties shall notify each other by sending a list of authorized personnel in accordance with national laws and regulations. Such list can not be valid for more than twelve months. Once the list has been approved, visits may be arranged directly according to national laws and regulations.

5. Classified Information acquired by a visitor shall be considered as Classified Information received under this Agreement.

ARTICLE 12 BREACH OF SECURITY

1. The National Security Authorities shall without undue delay inform each other in writing of any breach of security or suspicion thereof.
2. The National Security Authority of the Party where the breach of security has occurred, shall investigate the incident without undue delay. The National Security Authority of the other Party shall, if required, cooperate in the investigation.
3. In any case, the National Security Authority of the Recipient Party shall inform the National Security Authority of the Originating Party in writing about the circumstances of the breach of security, the extent of the damage, the measures adopted for its mitigation and the outcome of the investigation.
4. When the breach of security has occurred in a third Party, the National Security Authority which has released the Classified Information to the Third Party shall take the possible actions to ensure that the measures foreseen in this Article will be applied.

ARTICLE 13 EXPENSES

The implementation of this Agreement does not include any cost. Should any cost occur each Party shall bear its own costs.

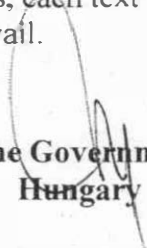
ARTICLE 14 FINAL PROVISIONS

1. This Agreement is concluded for an indefinite period of time. This Agreement shall enter into force on the first day of the second month following the date of receipt of the last of notifications between the Parties, through diplomatic channels, stating that the national legal requirements for this Agreement to enter into force have been fulfilled.
2. This Agreement may be amended on the basis of the mutual agreement of the Parties in writing. Such amendments shall enter into force in accordance with Paragraph 1 of this Article.
3. Each Party is entitled to terminate this Agreement in writing at any time. In such a case, the validity of this Agreement shall expire after six months following the day on which the other Party receives the written notice of the termination.
4. Regardless of the termination of this Agreement, all Classified Information exchanged or generated under this Agreement shall be protected in accordance with the provisions set forth herein until the Originating Party dispenses the Recipient Party from this obligation in writing.
5. Any dispute regarding the interpretation or implementation of this Agreement shall be resolved by consultations and negotiations between the Parties, without recourse to outside jurisdiction.

6. With the entry into force of this Agreement, the Agreement between the Government of the Republic of Hungary and the Government of the Italian Republic on the mutual protection of Classified Information signed on the 20th March 2003 shall expire.

In witness of which, the undersigned, duly authorised to this effect, have signed this Agreement.

Done in Budapest on November 26th, 2015 in two originals, in Hungarian, Italian and English languages, each text being equally authentic. In case of different interpretation the English text shall prevail.


**For the Government of
Hungary**

**For the Government of the Italian
Republic**

