2025. évi ... törvény

a Magyarország Kormánya és a Brazil Szövetségi Köztársaság Kormánya között a minősített adatok cseréjéről és kölcsönös védelméről szóló egyezmény kihirdetéséről

[1] Magyarország külpolitikájának alapvető célja, hogy elősegítse az ország nemzetközi súlyának növekedését, kultúrájának megismertetését, valamint a gazdasági és társadalmi modernizációt.
[2] Magyarország elkötelezett a Magyarország és a Brazil Szövetségi Köztársaság közötti kétoldalú kapcsolataikban a kölcsönös tisztelet alapján történő együttműködés iránt.
[3] A Felek közös szándéka a kicserélt vagy keletkezett minősített adatok védelmének biztosítása a védelmi, az energetikai, valamint a tudományos és technológiai területeken.
[4] A fenti célok elérése érdekében az Országgyűlés a következő törvényt alkotja:

1. §

Az Országgyűlés e törvénnyel felhatalmazást ad a Magyarország Kormánya és a Brazil Szövetségi Köztársaság Kormánya között a minősített adatok cseréjéről és kölcsönös védelméről szóló egyezmény (a továbbiakban: Egyezmény) kötelező hatályának elismerésére.

2. §

Az Országgyűlés az Egyezményt e törvénnyel kihirdeti.

3. §

(1) Az Egyezmény hiteles magyar nyelvű szövegét az 1. melléklet tartalmazza.

(2) Az Egyezmény hiteles angol nyelvű szövegét a 2. melléklet tartalmazza.

4. §

(1) Ez a törvény – a (2) bekezdésben foglalt kivétellel – a kihirdetését követő napon lép hatályba.

(2) A 2. § és a 3. §, valamint az 1. melléklet és a 2. melléklet az Egyezmény 14. CIKK 14.1 pontjában meghatározott időpontban lép hatályba.

(3) Az Egyezmény, a 2. §, a 3. §, valamint az 1. melléklet és a 2. melléklet hatálybalépésének naptári napját a külpolitikáért felelős miniszter annak ismertté válását követően a Magyar Közlönyben haladéktalanul közzétett közleményével állapítja meg.

5. §

Az e törvény végrehajtásához szükséges intézkedésekről a minősített adatok védelmének szakmai felügyeletéért felelős miniszter gondoskodik.

1. melléklet a 2025. évi … törvényhez

EGYEZMÉNY MAGYARORSZÁG KORMÁNYA ÉS A BRAZIL SZÖVETSÉGI KÖZTÁRSASÁG KORMÁNYA KÖZÖTT A MINŐSÍTETT ADATOK CSERÉJÉRŐL ÉS KÖLCSÖNÖS VÉDELMÉRŐL

Magyarország Kormánya és a Brazil Szövetségi Köztársaság Kormánya (a továbbiakban együttesen: a „Felek”, külön-külön: a „Fél”),
elismerve a Felek közötti kölcsönös együttműködés jelentőségét,
felismerve, hogy a Felek közötti hatékony együttműködés során szükség lehet minősített adatok cseréjére,
elismerve, hogy azonos szintű védelmet biztosítanak a minősített adatok számára,
kívánatosnak tartva, hogy a közöttük vagy a joghatóságuk alá tartozó jogi személyek és természetes személyek között kicserélt minősített adatok megfelelő védelemben részesüljenek,
kölcsönösen tiszteletben tartva a nemzeti érdekeket és a biztonságot, az alábbiakban állapodtak meg:

1. CIKK
AZ EGYEZMÉNY CÉLJA ÉS TÁRGYA

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

1.2 Jelen Egyezmény nem érinti a Feleknek más két- vagy többoldalú szerződésből eredő kötelezettségeit, beleértve a minősített adat cseréjét és kölcsönös védelmét szabályozó megállapodásokat is.

2. CIKK
FOGALOMMEGHATÁROZÁSOK

Jelen Egyezmény alkalmazásában:

a) **minősített adat biztonságának megsértése:** olyan tett vagy mulasztás, amely jelen Egyezménnyel vagy a Felek rájuk vonatkozó saját, nemzeti jogszabályainak és egyéb szabályainak rendelkezéseivel ellentétes, és amely a minősített adat jogosulatlan nyilvánosságra hozatalát, elvesztését, megsemmisülését, jogosulatlan felhasználását, megszerzését vagy bármilyen más típusú veszélyeztetését eredményezheti;

b) **minősített szerződés:** olyan szerződés vagy szerződéskötést megelőző tárgyalások, amelyek minősített adatot tartalmaznak, vagy amelyek alapján minősített adathoz történő hozzáférés, annak keletkeztetése, felhasználása, kezelése vagy továbbítása szükséges;

c) **minősített adat**: megjelenési formájától vagy természetétől függetlenül, minden olyan adat, amelyet bármelyik Fél nemzeti jogszabályai és egyéb szabályai szerint védelemben kell részesíteni a minősített adat biztonságának megsértésével szemben és amelyet ennek megfelelően minősítettek,

d) **szerződő/alvállalkozó:** az a természetes személy vagy jogi személy, aki a minősített szerződés megkötésére a nemzeti jogszabályok és egyéb szabályok szerint jogképességgel rendelkezik;

e) **telephely biztonsági tanúsítvány:** a nemzeti biztonsági hatóság azon döntése, amely szerint a szerződő/alvállalkozó – a nemzeti jogszabályokkal és egyéb szabályokkal összhangban – rendelkezik a minősített adatok védelmének biztosítására vonatkozó képességgel, annak érdekében, hogy szerződéskötést megelőző tevékenységben vagy minősített szerződésben vegyen részt;

f) **nemzeti biztonsági hatóság:** az az állami szerv, amely jelen Egyezmény végrehajtásáért és felügyeletéért felelős;

g) **szükséges ismeret**: az a követelmény, amely alapján minősített adathoz való hozzáférés csak annak a személynek biztosítható, akinek az adott minősített adathoz való hozzáférés hivatali kötelessége vagy meghatározott feladata ellátásához igazoltan szükséges;

h) **átadó Fél:** az a Fél – beleértve a joghatósága alá tartozó jogi személyeket vagy természetes személyeket – amelyik a minősített adatot átadja;

i) **személyi biztonsági tanúsítvány**: a nemzeti biztonsági hatóság azon döntése, amely megállapítja, hogy egy személy a nemzeti jogszabályokkal és egyéb szabályokkal összhangban meghatározott szintű minősített adatokhoz hozzáférhet;

j) **projekt biztonsági utasítás:** egy adott projektre alkalmazott biztonsági előírások/eljárások összesége;

k) **átvevő Fél:** az a Fél, – beleértve a joghatósága alá tartozó jogi személyeket vagy természetes személyeket – amelyik a minősített adatot átveszi;

l) **harmadik fél:** bármely olyan állam, – beleértve a joghatósága alá tartozó jogi személyeket vagy természetes személyeket – vagy nemzetközi szervezet, amely nem részese jelen Egyezménynek.

3. CIKK
NEMZETI BIZTONSÁGI HATÓSÁGOK

3.1 A Felek nemzeti biztonsági hatóságai a következők:

Magyarországon:
Nemzeti Biztonsági Felügyelet (National Security Authority)

A Brazil Szövetségi Köztársaságban:
Gabinete de Segurança Institucional da Presidência da República Federativa do Brasil (Institutional Security Cabinet of the Presidency of the Federative Republic of Brazil)

3.2 A nemzeti biztonsági hatóságok egymás rendelkezésére bocsátják hivatalos elérhetőségeiket és tájékoztatják egymást a nemzeti biztonsági hatóságokkal kapcsolatos valamennyi későbbi változásról.

3.3 A nemzeti biztonsági hatóságok nevében bekövetkező változások nem tekintendőek ezen Egyezmény módosításának. A nemzeti biztonsági hatóságok írásban tájékoztatják egymást e változásokról.

4. CIKK
MINŐSÍTÉSI SZINTEK ÉS JELÖLÉSEIK

4.1 A jelen Egyezmény alapján átadott minősített adatot a Felek jogszabályainak és egyéb szabályainak megfelelően megfelelő minősítési szinttel kell ellátni.

4.2 A Felek vállalják, hogy védik az egymás között kicserélt minősített adatot, és megállapodnak abban, hogy az egyes biztonsági minősítési szintek az alábbiak szerint feleltethetők meg egymásnak:

Magyarországon	**A Brazil Szövetségi Köztársaságban**	**Angol nyelvi megfelelőjük**
„Szigorúan titkos!”	ULTRASSECRETO	TOP SECRET
„Titkos!”	SECRETO	SECRET
„Bizalmas!”	RESERVADO	CONFIDENTIAL
„Korlátozott terjesztésű!”	NINCS EGYENÉRTÉKŰ	RESTRICTED

4.3 A „Korlátozott terjesztésű!” /RESTRICTED minősítési szintű, Magyarország által átadott minősített adatot ugyanúgy kell védeni, mint a „RESERVADO” minősítési szintű minősített adatot a Brazil Szövetségi Köztársaságban.

5. CIKK
MINŐSÍTETT ADATHOZ VALÓ HOZZÁFÉRÉS

Jelen Egyezmény alapján minősített adathoz kizárólag olyan természetes személyek kaphatnak hozzáférést, akik a szükséges ismeret elvének megfelelnek, részükre a megfelelő személyi biztonsági tanúsítványt kibocsátották és a rájuk vonatkozó nemzeti jogszabályoknak és egyéb szabályoknak megfelelően felhatalmazást kaptak a minősített adathoz való hozzáférésre.

6. CIKK
A MINŐSÍTETT ADATOK VÉDELMÉRE VONATKOZÓ ALAPELVEK

6.1 Az átadó Fél:

a) biztosítja, hogy a minősített adaton a nemzeti jogszabályainak és egyéb szabályainak megfelelő minősítési szint feltüntetésre kerüljön;
b) írásban tájékoztatja az átvevő Felet az átadott vagy keletkeztetett minősített adat felhasználásával kapcsolatos esetleges különleges feltételekről;
c) haladéktalanul írásban tájékoztatja az átvevő Felet az adat minősítési szintjében vagy érvényességi idejében bekövetkezett változásokról.

6.2 Az átvevő Fél:

a) biztosítja, hogy a minősített adaton feltüntetésre kerüljön jelen Egyezmény 4. cikke alapján meghatározott egyenértékű minősítési szint;
b) ugyanolyan szintű védelemben részesíti a minősített adatot, mint amelyet a saját,

azonos minősítési szintű nemzeti minősített adata számára biztosít;

c) mindaddig biztosítja a minősített adat minősítési szintjének megfelelő védelmet, amíg az átadó Féltől az átvett minősített adat minősítésének megszüntetéséről, illetve minősítési szintjének vagy érvényességi idejének megváltoztatásáról írásban tájékoztatást nem kap;

d) biztosítja, 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 és az átadó Fél által előírt korlátozásoknak megfelelően használja fel, betartva az átadó Fél által meghatározott, az adat felhasználásával kapcsolatos átadási feltételeket.

f) biztosítja a megfelelő adminisztratív biztonsági intézkedések bevezetésével a minősített adat nyomon követhetőségét, bizalmasságát, sértetlenségét és rendelkezésre állását.

7. CIKK
BIZTONSÁGI EGYÜTTMŰKÖDÉS

7.1 Az összeegyeztethető szintű biztonsági követelmények fenntartása érdekében a nemzeti biztonsági hatóságok a másik Fél megkeresésére tájékoztatják egymást a minősített adatok védelmével kapcsolatos nemzeti jogszabályokról és egyéb szabályokról, valamint mindezek gyakorlati alkalmazásáról.

7.2 Megkeresés esetén a nemzeti biztonsági hatóságok, összhangban a nemzeti jogszabályaik és egyéb szabályaik rendelkezéseivel, kölcsönösen segítséget nyújtanak egymásnak a személyi biztonsági tanúsítványokkal és a telephely biztonsági tanúsítványokkal kapcsolatos eljárások során.

7.3 A Felek nemzeti jogszabályaik és egyéb szabályaik rendelkezéseivel összhangban elismerik a másik Fél által kibocsátott személyi biztonsági tanúsítványokat és telephely biztonsági tanúsítványokat. Mindezek során a jelen Egyezmény 4. Cikkében foglaltak alkalmazandók.

7.4 A nemzeti biztonsági hatóságok haladéktalanul értesítik egymást az elismert személyi biztonsági tanúsítványokkal és telephely biztonsági tanúsítványokkal kapcsolatos változásokról, különösen azok visszavonásáról.

7.5 Amennyiben a Felek közötti együttműködés során minősített adat keletkezik, a minősítési szint és az érvényességi idő meghatározása, ezek megváltoztatása vagy a minősítés megszüntetése a Felek közös egyetértésével, nemzeti jogszabályaikkal összhangban történhet.

7.6 Jelen Egyezmény alapján megvalósuló együttműködés angol nyelven történik. A nemzeti biztonsági hatóságok e megállapodással kapcsolatban végrehajtási megállapodásokat köthetnek.

8. CIKK
MINŐSÍTETT SZERZŐDÉSEK

8.1 A minősített szerződéseket a Felek saját nemzeti jogszabályai és egyéb szabályai alapján kell megkötni és teljesíteni. A nemzeti biztonsági hatóságok megkeresésre igazolják, hogy a szerződéskötést megelőző tárgyalásokban vagy a minősített szerződések teljesítésében részt vevő javasolt szerződők/alvállalkozók rendelkeznek megfelelő személyi biztonsági tanúsítvánnyal vagy telephely biztonsági tanúsítvánnyal.

8.2 A nemzeti biztonsági hatóság a minősített adatok folyamatos védelmének biztosítása céljából biztonsági ellenőrzés lefolytatását kérheti a másik Fél nemzeti biztonsági hatóságától a másik Fél országának területén működő, minősített szerződéssel érintett létesítményben.

8.3 A minősített szerződések kötelező részét képezi a projekt biztonsági utasítás, amely a biztonsági követelményeket és a szerződés egyes elemeinek minősítésével kapcsolatos rendelkezéseket határozza meg. A projekt biztonsági utasítás másolatát továbbítani szükséges azon Fél nemzeti biztonsági hatósága részére, amelynek joghatósága alatt a minősített szerződés végrehajtása történik.

8.4 Az alvállalkozókra ugyanazokat a biztonsági intézkedéseket kell alkalmazni, mint a szerződőre.

9. CIKK
A MINŐSÍTETT ADAT TOVÁBBÍTÁSA

9.1 A minősített adat továbbítása az átadó Fél nemzeti jogszabályainak és egyéb szabályainak rendelkezései szerint diplomáciai úton, vagy a nemzeti biztonsági hatóságok által előzetesen írásban, közösen meghatározott egyéb biztonságos módon történik.

9.2 A Felek elektronikus úton a nemzeti biztonsági hatóságok által írásban jóváhagyott biztonsági eljárásrenddel összhangban továbbíthatnak minősített adatot.

9.3 A *„Szigorúan titkos!” / ULTRASSECRETO / TOP SECRET* minősítésű minősített adatok elektronikus úton történő átadása és továbbítása elektronikus rendszeren keresztül tilos.”

10. CIKK
A MINŐSÍTETT ADAT SOKSZOROSÍTÁSA, KIVONATOLÁSA, FORDÍTÁSA ÉS MEGSEMMISÍTÉSE

10.1 A minősített adat sokszorosítását, kivonatolását, fordítását és megsemmisítését az átadó Fél korlátozhatja vagy kizárhatja.

10.2 Jelen Egyezmény alapján átadott minősített adatról készült sokszorosított példányon, kivonatokon és fordításokon fel kell tüntetni a megfelelő minősítési szintet és egyéb jelölést, az így készült adatot pedig ugyanolyan védelemben kell részesíteni, mint az eredeti minősített adatot. A sokszorosított példányok számát a hivatalos célból szükséges minimumra kell korlátozni.

10.3 Jelen Egyezmény alapján átadott minősített adatról készült fordításokon a fordítás nyelvén fel kell tüntetni, hogy az az átadó Fél minősített adatát tartalmazza.

10.4 Jelen Egyezmény alapján átadott *„Szigorúan titkos!” / ULTRASSECRETO / TOP SECRET* minősítésű adat sokszorosítása, kivonatolása vagy fordítása kizárólag az átadó Fél előzetes írásbeli hozzájárulásával történhet.

10.5 Jelen Egyezmény alapján átadott *„Szigorúan titkos!” / ULTRASSECRETO / TOP SECRET* minősítésű adat nem semmisíthető meg és az átadó Fél részére vissza kell küldeni, ha az átvevő Félnek megítélése szerint már nincs szüksége rá.

10.6 Olyan válsághelyzet esetén, amely lehetetlenné teszi a minősített adat védelmét vagy visszajuttatását az átadó Félnek, a minősített adatot haladéktalanul meg kell semmisíteni. A minősített adat megsemmisítésről az átvevő Fél nemzeti biztonsági hatósága haladéktalanul, írásban értesíti az átadó Fél nemzeti biztonsági hatóságát.

11. CIKK
LÁTOGATÁSOK

11.1 Személyi biztonsági tanúsítványt igénylő látogatásra a fogadó Fél nemzeti biztonsági hatóságának előzetes írásbeli hozzájárulása alapján kerülhet sor.

11.2 A látogatást kezdeményező Fél nemzeti biztonsági hatósága a fogadó Fél nemzeti biztonsági hatóságának a tervezett látogatásról legalább harminc (30) nappal a látogatás időpontja előtt látogatási kérelmet küld. Sürgős esetben, a nemzeti biztonsági hatóságok előzetes egyeztetését követően a látogatásra vonatkozó megkeresés a látogatás kezdetéhez közelebbi időpontban is benyújtható.

11.3 A látogatási kérelemnek 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 intézménynek 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, beleértve a látogatással érintett legmagasabb minősítési szintű minősített adat minősítési szintjét;
f) a meglátogatandó létesítmény neve és címe, valamint a kapcsolattartójának neve, telefonszáma/ fax száma, e-mail címe;
g) dátum, aláírás és a nemzeti biztonsági hatóság hivatalos pecsétjének lenyomata.

11.4 A nemzeti biztonsági hatóságok közösen meghatározhatják a visszatérő látogatásra jogosult személyek listáját. A visszatérő látogatások további részleteit a nemzeti biztonsági hatóságok állapítják meg.

11.5 A látogató által megismert minősített adatot úgy kell tekinteni, mint a jelen Egyezmény alapján átadott minősített adatot.

12. CIKK
A MINŐSÍTETT ADAT BIZTONSÁGÁNAK MEGSÉRTÉSE

12.1 A nemzeti biztonsági hatóságok késedelem nélkül írásban tájékoztatják egymást a minősített adat biztonságának megsértéséről vagy annak gyanúja esetén.

12.2 Annak a Félnek a nemzeti biztonsági hatósága, ahol a minősített adat biztonságának megsértése bekövetkezett köteles késedelem nélkül gondoskodni az esemény kivizsgálása iránt. A másik Fél nemzeti biztonsági hatóságától a vizsgálat során szükség esetén tájékoztatás kérhető az eseménnyel kapcsolatban.

12.3 Az átvevő Fél nemzeti biztonsági hatósága minden esetben írásban tájékoztatja az átadó Fél nemzeti biztonsági hatóságát a minősített adat biztonságának megsértésével kapcsolatos körülményekről, a kár mértékéről, a kár enyhítése érdekében megtett intézkedésekről, valamint a vizsgálat eredményéről.

13. CIKK
KÖLTSÉGEK VISELÉSE

A Felek maguk viselik a jelen Egyezmény végrehajtásával összefüggésben felmerült költségeiket.

14. CIKK
ZÁRÓ RENDELKEZÉSEK

14.1 Jelen Egyezmény határozatlan időre jön létre. Jelen Egyezmény a Felek által az Egyezmény hatálybalépéséhez szükséges belső jogi feltételek teljesüléséről diplomáciai úton küldött, utolsó értesítés kézhezvételének napját követő második hónap első napján lép hatályba.

14.2 Jelen Egyezmény a Felek kölcsönös egyetértésével írásban módosítható. A módosítások hatálybalépésével kapcsolatban a jelen Cikk 14.1 pontjában foglaltak az irányadók.

14.3 Bármelyik Fél jogosult jelen Egyezményt bármikor írásban, diplomáciai úton felmondani. Felmondás esetén az Egyezmény a felmondásról szóló írásbeli értesítés másik Fél általi kézhezvételének napjától számított hat hónap elteltével hatályát veszti.

14.4 Az Egyezmény megszűnésétől függetlenül az annak alapján átadott vagy keletkezett minősített adatokat az Egyezményben meghatározott rendelkezések szerint kell védelemben részesíteni, mindaddig, amíg az adat minősített.

14.5 Jelen Egyezmény végrehajtásából vagy értelmezéséből fakadó vitákat a Felek egymás közötti egyeztetés vagy tárgyalás útján, külső igazságszolgáltatási fórum igénybevétele nélkül rendezik.

14.6 A Felek közötti vitarendezési eljárásokat a bizalmasság elvének megfelelően kell lefolytatni.

Fentiek tanúbizonyságául, az alulírott és az erre felhatalmazott megbízottak jelen Egyezményt aláírásukkal látták el.

Készült ……-ben, ……..-én, két eredeti példányban, magyar, portugál és angol nyelven, valamennyi szöveg egyaránt hiteles. Eltérés esetén az angol nyelvű szöveg az irányadó.

……	……
Magyarország Kormánya részéről	A Brazil Szövetségi Köztársaság Kormánya részéről

AGREEMENT BETWEEN THE GOVERNMENT OF HUNGARY AND THE GOVERNMENT OF THE FEDERATIVE REPUBLIC OF BRAZIL ON THE EXCHANGE AND MUTUAL PROTECTION OF CLASSIFIED INFORMATION

The Government of Hungary and the Government of the Federative Republic of Brazil (hereinafter collectively referred to as the "Parties" and individually as the Party),
recognising the importance of mutual cooperation between the Parties,
realising that good cooperation may require exchange of Classified Information between the Parties,
recognising that they ensure equivalent protection for the Classified Information,
wishing to ensure the protection of Classified Information exchanged between them or between the legal entities or individuals under their jurisdiction,
have, in mutual respect for national interests and security, agreed upon the following:

ARTICLE 1
OBJECTIVE AND APPLICABILITY OF THE AGREEMENT

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

1.2 This Agreement shall not affect the obligation of the Parties under any other bilateral or multilateral treaty, including any agreements governing exchange and mutual protection of Classified Information.

ARTICLE 2
DEFINITIONS

For the purpose of this Agreement:

a) **"Breach of Security**" means an act or an omission which is contrary to this Agreement or to the national laws and regulations of the Parties, the result of which may lead to unauthorized disclosure, loss, destruction, misappropriation, access or any other type of compromise of Classified Information;
b) **"Classified Contract"** means a contract, or pre-contractual negotiations, which contains Classified Information or which involves access to, or the generation, use, management or transmission of Classified Information.
c) **"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;
d) **"Contractor/Sub-contractor"** means a legal entity or an individual possessing the legal capacity to conclude Classified Contracts in accordance with the national laws and regulations;
e) **"Facility Security Clearance"** means a document issued by the national security authority which determines the capability of a Contractor/Sub-contractor to protect Classified Information in order to participate in pre-contractual activities or perform Classified Contracts, in accordance with the respective national legislation;
f) "**National Security Authority**" means the state authority responsible for the application

and supervision of this Agreement;

g) **"Need-to-Know**" means the principle, according to which access to Classified Information may only be granted to a person who has a verified need to access the Classified Information in connection with his/her official duties or for the performance of a specific task;
h) **"Originating Party"** means the Party including the legal entities or individuals under its jurisdiction, which releases Classified Information;
i) **"Personnel Security Clearance"** means a document issued by a national security authority in accordance with the respective national legislation determining that access to information of a certain classification level may be granted to an individual;
j) **"Project Security Instruction"** means a compilation of security regulations/procedures which are applied to a specific project;
k) **"Recipient Party"** means the Party including the legal entities or individuals under its jurisdiction, which receives Classified Information;
l) **"Third Party"** means any state including the legal entities or individuals under its jurisdiction or international organization not being a Party to this Agreement.

ARTICLE 3
NATIONAL SECURITY AUTHORITIES

3.1 The National Security Authorities of the Parties are:

In Hungary:
Nemzeti Biztonsági Felügyelet (National Security Authority)
In the Federative Republic of Brazil:
Gabinete de Segurança Institucional da Presidência da República Federativa do Brasil (Institutional Security Cabinet of the Presidency of the Federative Republic of Brazil)

3.2 The National Security Authorities shall provide each other with official contact details and shall inform each other of any subsequent changes regarding to the National Security Authorities.

3.3 Changes in the names of the National Security Authorities shall not constitute modification of this Agreement. The National Security Authorities shall inform each other in writing about such changes.

ARTICLE 4
CLASSIFICATION LEVELS AND MARKINGS

4.1 Any Classified Information released under this Agreement shall be marked with the appropriate security classification level in accordance with the Parties' respective laws and regulations.

4.2 The Parties undertake to protect Classified Information exchanged between them and agree that the following security classification levels shall be equivalent:

In Hungary	In the Federative Republic of Brazil	Equivalent in English language
„Szigorúan titkos!"	ULTRASSECRETO	TOP SECRET

„Titkos!”	SECRETO	SECRET
„Bizalmas!”	RESERVADO	CONFIDENTIAL
„Korlátozott terjesztésű!”	NO EQUIVALENCE	RESTRICTED

4.3 Classified Information exchanged by Hungary with the Classification Level of „Korlátozott terjesztésű!”/RESTRICTED/ shall be protected the same as the Classified Information with the Classification Level of “RESERVADO” in the Federative Republic of Brazil.

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, who have been issued an appropriate Personnel Security Clearance and who are duly authorized in accordance with the national laws and regulations of the respective Party.

ARTICLE 6
SECURITY PRINCIPLES

6.1 The Originating Party shall:

a) ensure that Classified Information is marked with appropriate classification markings in accordance with its national laws and regulations;
b) inform the Recipient Party in writing of any special conditions regarding the handling of the Classified Information exchanged or generated;
c) inform the Recipient Party in writing without undue delay of any subsequent changes in the classification level or in the term of validity.

6.2 The Recipient Party shall:
a) ensure that Classified Information is marked with equivalent classification marking in accordance with Article 4 of this Agreement;
b) ensure the same level of protection to Classified Information as ensured to its own Classified Information of equivalent classification level;
c) ensure protection of the Classified Information equivalent to its classification level until the written notification from the Originating Party about the declassification or the change of the classification level or validity of the Classified Information;
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 any restriction given by the Originating Party;
f) ensure the traceability, confidentiality, integrity and availability of Classified Information by implementing appropriate administrative security measures.

ARTICLE 7
SECURITY COOPERATION

7.1 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 stemming from their implementation.

7.2 On request, the National Security Authorities shall, in accordance with their national laws and regulations, assist each other during the Personnel Security Clearance procedures and Facility Security Clearance procedures.

7.3 Within the scope of this Agreement, the Parties shall in accordance with their national laws and regulations, recognize the Personnel Security Clearances and Facility Security Clearances issued by the other Party. Article 4 of this Agreement shall apply accordingly.

7.4 The National Security Authorities shall promptly notify each other about changes in the recognized Personnel Security Clearances and Facility Security Clearances, especially in case of their withdrawal.

7.5 When Classified Information is generated in the course of cooperation between the Parties, the assignment of a classification level, the validity of the classification level, their change or the declassification shall be made upon common consent of the Parties, in accordance with their national legislation.

7.6 The cooperation under this Agreement shall be effected in the English language. The National Security Authorities may conclude implementing arrangements in relation with this Agreement.

ARTICLE 8
CLASSIFIED CONTRACTS

8.1 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/Subcontractors participating in pre-contractual negotiations or in the implementation of Classified Contracts have appropriate Personnel Security Clearance or Facility Security Clearance.

8.2 The National Security Authority may request its counterpart to conduct a security inspection at a facility located in the territory of the other Party to ensure continuing protection of Classified Information.

8.3 Classified Contracts shall contain Project Security Instructions on the security requirements and on the 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.

8.4 For the sub-contractors, the same security measures shall be applied as for the contractors.

ARTICLE 9
TRANSFER OR TRANSMISSION OF CLASSIFIED INFORMATION

9.1 Classified Information shall be transferred between the Parties through diplomatic channels or through other secure channels mutually agreed upon in advance in writing by their National Security Authorities in accordance with the Parties' respective laws and regulations.

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

9.3 Electronic exchange and transmission of Classified Information marked as *„Szigorúan titkos!" / ULTRASSECRETO / TOP SECRET* through communication and information systems is prohibited.

ARTICLE 10
REPRODUCTION, EXTRACTION, TRANSLATION AND DESTRUCTION OF CLASSIFIED INFORMATION

10.1 The reproduction, extraction, translation and destruction of Classified Information may be restricted or excluded by the Originating Party.

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

10.3 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.

10.4 Classified Information released under this Agreement marked *„Szigorúan titkos!" / ULTRASSECRETO / TOP SECRET* shall be reproduced, extracted or translated only upon the prior written consent of the Originating Party.

10.5 Classified Information released under this Agreement marked *„Szigorúan titkos!" / ULTRASSECRETO / TOP SECRET* shall not be destroyed and shall be returned to the Originating Party after it is no longer considered necessary by the Recipient Party.

10.6 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 as soon as possible.

ARTICLE 11
VISITS

11.1 Visits requiring a Personal Security Clearance shall be subject to the prior written consent of the National Security Authority of the host Party.

11.2. 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 thirty (30) 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.

11.3 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 organization represented;
c) visitor's Personnel Security Clearance 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 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.

11.4 The National Security Authorities may agree on a list of visitors entitled to recurring visits. The National Security Authorities shall agree on the further details of the recurring visits.

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

ARTICLE 12
BREACH OF SECURITY

12.1 The National Security Authorities shall inform each other in writing without undue delay of any Breach of Security or suspicion thereof.

12.2 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 can be requested for notification about the incident during the investigation.

12.3 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.

ARTICLE 13
EXPENSES

Each Party shall bear its own expenses incurred in the course of the implementation of this Agreement.

ARTICLE 14
FINAL PROVISIONS

14.1 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.

14.2 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.

14.3 Each Party is entitled to terminate this Agreement in writing, through diplomatic channels, at any time. In such a case, the validity of this Agreement shall expire after six (6)

months following the day on which the other Party receives the written notice of the termination.

14.4 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 for as long as the Classified Information remains classified.

14.5 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.

14.6 Dispute settlement procedures between both Parties shall be conducted based on the principle of confidentiality.

In witness whereof, the undersigned, duly authorized to this effect, have signed this Agreement.

Done in ..... on ..... in two originals, in Hungarian, Portuguese and English languages, each text being equally authentic. In case of divergence of interpretation the English text shall prevail.

……	……
for the Government of Hungary	for the Government of the Federative Republic of Brazil