MAGYARORSZÁG KORMÁNYA

T/9777. számú

törvényjavaslat

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

Előadó: **Dr. Navracsics Tibor**
közigazgatási és igazságügyi miniszter

Budapest, 2013. január

2013. évi … törvény

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

1. §

Az Országgyűlés e törvénnyel felhatalmazást ad a Magyarország Kormánya és a Francia 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. §

Az Egyezmény hiteles magyar és francia nyelvű szövege a következő:

„EGYEZMÉNY MAGYARORSZÁG KORMÁNYA ÉS A FRANCIA KÖZTÁRSASÁG KORMÁNYA KÖZÖTT A MINŐSÍTETT ADATOK CSERÉJÉRŐL ÉS KÖLCSÖNÖS VÉDELMÉRŐL

Magyarország Kormánya és a Francia Köztársaság Kormánya (a továbbiakban együtt: Felek)

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

Kívánatosnak tartva a Felek, valamint a joghatóságuk alá tartozó jogi és természetes személyek közötti együttműködés során kicserélt vagy keletkezett minősített adatok védelmét,

Az alábbiakban állapodtak meg:

1. Cikk
Az Egyezmény tárgya

1. Jelen Egyezmény szabályozza a Felek, valamint a joghatóságuk alá tartozó természetes és jogi személyek közötti együttműködés során továbbított vagy keletkezett valamennyi minősített adat cseréjét.

2. Az Egyezmény nem érinti a Felek egyéb, két-, vagy többoldalú szerződés alapján fennálló kötelezettségeit, beleértve ebbe mindazon megállapodásokat, 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 szerint védelemben kell részesíteni a jogosulatlan nyilvánosságra hozatallal vagy jogosulatlan megváltoztatással és kezeléssel szemben, s amelyet ennek megfelelően minősítettek;

b) a „**Minősített Szerződés**” olyan szerződést jelent, amely minősített adatot tartalmaz vagy amely alapján minősített adathoz való hozzáférés szükséges;

c) a „**Szerződő Fél**” minden, minősített szerződés tárgyalására és megkötésére jogképességgel rendelkező személy;

d) a „**Nemzeti Biztonsági Felügyelet**” a Felek jelen Egyezmény végrehajtására és annak ellenőrzésére hatáskörrel rendelkező nemzeti hatósága;

e) a „**Hatáskörrel Rendelkező Hatóság**” a Felek nemzeti joga alapján jelen Egyezmény végrehajtására az érintett területen hatáskörrel rendelkező valamennyi hatóság, beleértve a kijelölt biztonsági hatóságokat valamint az egyéb szervezeteket is;

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

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

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

i) a „**Szükséges Ismeret**” követelményének megfelelően a minősített adatokhoz csak az a személy férhet hozzá, aki igazolta, hogy a minősített adathoz történő hozzáférése – az Átvevő Fél részére történő adatcsere céljával összhangban álló – feladata ellátásához szükséges;

j) a „**Személy**” minden természetes vagy jogi személy;

k) a „**Biztonsági Tanúsítvány**” egy olyan, vizsgálaton alapuló jóváhagyó döntés, amely a Felek hatályos joga alapján, egy személy lojalitását, megbízhatóságát és egyéb biztonsági szempontoknak való megfelelését igazolja. Ez a döntés teszi lehetővé, hogy egy személy a minősített adatokhoz történő hozzáférésre és azok feldolgozására engedélyt kapjon. A természetes személy részére kiadott Biztonsági Tanúsítvány a Személyi Biztonsági Tanúsítvány, a jogi személy részére kiadott a Telephely Biztonsági Tanúsítvány.

3. Cikk
A hatáskörrel rendelkező hatóságok

1. A Feleknek a minősített adatok védelméért, valamint jelen Egyezmény végrehajtásáért felelős, hatáskörrel rendelkező Nemzeti Biztonsági Felügyeletei a következők:

Magyarországon:

Nemzeti Biztonsági Felügyelet
H-1024 Budapest, Szilágyi Erzsébet fasor 11/B.

A Francia Köztársaságban:

Secrétariat general de la defense et de la sécurité nationale (SGDSN)
51 boulevard de La Tour-Maubourg
75007 PARIS

2. A Nemzeti Biztonsági Felügyeletek kölcsönösen tájékoztatják egymást a hivatalos elérhetőségi adatokról, illetve az ezen adatokkal kapcsolatos változásokról.

3. A Felek diplomáciai úton tájékoztatják egymást a Nemzeti Biztonsági Felügyeletet vagy az egyéb Hatáskörrel Rendelkező Hatóságokat érintő minden változásról.

4. Cikk
Minősítési szintek megfeleltetése

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

Magyarországon	**A Francia Köztársaságban**
„SZIGORÚAN TITKOS!”	TRES SECRET DEFENSE
„TITKOS!”	SECRET DEFENSE
„BIZALMAS!”	CONFIDENTIEL DEFENSE

„KORLÁTOZOTT TERJESZTÉSŰ!”	DIFFUSION RESTREINTE

2. A Francia Köztársaság ugyanúgy kezeli és védi a Magyarország részéről átadott „Korlátozott terjesztésű!” minősített adatot, mint amilyen védelmet a hatályos joga alapján a „DIFFUSION RESTREINTE” megjelölésű védett, de nem minősített adatnak biztosít.

3. Magyarország ugyanúgy kezeli és védi a Francia Köztársaság részéről átadott „DIFFUSION RESTREINTE” megjelölésű védett, de nem minősített adatot, mint a hatályos joga alapján a „Korlátozott terjesztésű!” minősített adatot.

4. Amennyiben különös biztonsági okokból az Átadó Fél igényli, hogy csak a Felek kizárólagos állampolgárságával rendelkező személyek férhessenek hozzá a minősített adathoz, azt a ”Kizárólag francia vagy magyar állampolgársággal rendelkezők részére” vagy a“SPÉCIAL FRANCE – HONGRIE” kiegészítő jelöléssel látja el.

5. Cikk
Minősített adathoz való hozzáférés

„BIZALMAS!” / CONFIDENTIEL DEFENSE és magasabb minősítésű szintű, jelen Egyezmény hatálya alá tartozó minősített adathoz kizárólag olyan személyek jogosultak hozzáférni, akik megfelelnek a Szükséges Ismeret követelményének, és akik az adott Fél nemzeti jogszabályaival összhangban Személyi Biztonsági Tanúsítvánnyal rendelkeznek.

6. Cikk
Biztonsági alapelvek

1. Az Átadó Fél:
a) köteles biztosítani, hogy a minősített adaton a nemzeti jogszabályai szerinti megfelelő minősítési szint feltüntetésre kerüljön;
b) köteles tájékoztatni az Átvevő Felet a minősített adat felhasználásának esetleges feltételhez kötéséről;
c) haladéktalanul köteles tájékoztatni az Átvevő Felet az adat minősítésében bekövetkezett változásokról.

2. Az Átvevő Fél:
a) köteles az Átadó Féltől átvett minősített adaton saját nemzeti minősítési szintjét – a 4. Cikk alapján meghatározott megfelelő minősítési szinttel összhangban – feltüntetni;
b) ugyanolyan szintű védelemben köteles részesíteni a minősített adatot, mint amelyet a saját, azonos minősítési szintű minősített adata számára biztosít;
c) köteles biztosítani, hogy az Átadó Fél előzetes írásbeli hozzájárulása nélkül az átvett 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 kezelési előírásokat.

3. A minősített adat rendelkezésre állásának és ellenőrzésének biztosítása céljából a Felek minden olyan szervezeténél (intézményénél, gazdasági társaságánál), amely minősített adatot

készít, feldolgoz és/vagy tárol, olyan nyilvántartó rendszert kell működtetni, amely biztosítja a minősített adat átvételét, terjesztését, ellenőrzését, védelmét. A rendszert az érintett Fél Hatáskörrel Rendelkező Hatóságával akkreditáltatni kell.

4. Jelen Egyezmény hatálya alá tartozó valamennyi elektronikus minősített adat kezelésére használt kommunikációs és információs rendszert az érintett Fél Hatáskörrel Rendelkező Hatóságával akkreditáltatni kell.

7. Cikk
Biztonsági együttműködés

1. A hasonló szintű biztonsági követelmények fenntartása érdekében a Hatáskörrel Rendelkező Hatóságok a másik fél megkeresésére kötelesek egymást tájékoztatni a minősített adat védelmével kapcsolatos nemzeti jogszabályokról, valamint mindezek gyakorlati alkalmazásáról. A Hatáskörrel Rendelkező Hatóságok tájékoztatják továbbá egymást minden, a nemzeti jogszabályaikat érintő, jelen Egyezménnyel kapcsolatos lényeges változásról.

2. Megkeresés esetén a Hatáskörrel Rendelkező Hatóságok, összhangban a nemzeti jogszabályaik rendelkezéseivel, kölcsönösen segítséget nyújthatnak egymásnak a Személyi Biztonsági Tanúsítványokkal és a Telephely Biztonsági Tanúsítványokkal kapcsolatos eljárások során.

3. A Felek megkeresés esetén nemzeti jogszabályaik rendelkezéseivel összhangban elismerik a másik Fél által kibocsátott Személyi Biztonsági Tanúsítványokat és Telephely Biztonsági Tanúsítványokat.

4. A Hatáskörrel Rendelkező Hatóságok haladéktalanul értesítik egymást az elismert Személyi Biztonsági Tanúsítványokkal és a Telephely Biztonsági Tanúsítványokkal kapcsolatos változásokról, különösen azok visszavonásáról vagy szintjének csökkentéséről.

8. Cikk
Minősített Szerződések

1. A Minősített Szerződéseket a Felek saját nemzeti jogszabályai alapján kell megkötni és teljesíteni. A Hatáskörrel Rendelkező Hatóságok megkeresésre kötelesek megerősíteni, hogy az ajánlattevő és az előzetes szerződési tárgyalásokban vagy a Minősített Szerződések teljesítésében részt vevő természetes személyek rendelkeznek-e megfelelő Személyi Biztonsági Tanúsítvánnyal vagy Telephely Biztonsági Tanúsítvánnyal.

2. A Hatáskörrel Rendelkező Hatóságok kérelmezhetik, hogy a másik Fél biztonsági ellenőrzést folytasson le a területén működő létesítményben a minősített adat folyamatos védelmének biztosítása céljából.

3. Az a Hatáskörrel Rendelkező Hatóság, amelynek területén a szerződés végrehajtásra kerül, a Minősített Szerződés teljesesítés során köteles az átvett minősített adatnak az azonos minősítésű szintű, saját minősített adatáéval megegyező mértékű védelmét biztosítani és fenntartani.

4. A Minősített Szerződéseknek projekt biztonsági utasítást és minősítési útmutatót is kell tartalmazniuk. A biztonsági utasításnak összhangban kell lennie az Átadó Fél Hatáskörrel Rendelkező Hatóságának biztonsági utasításaival, és meg kell benne határozni, mely adatokat és milyen minősítési szinten kell az Átvevő Félnek védenie. A projekt biztonsági utasítás és a minősítési útmutató másolatát azon Fél Hatáskörrel Rendelkező Hatósága részére kell továbbítani, amelynek joghatósága alatt a Minősített Szerződés végrehajtása történik.

5. A Szerződő Fél minősített adatok védelméért való felelőssége legalább az alábbi kötelezettségeket foglalja magában:

a) a minősített adathoz csak olyan személyek férhetnek hozzá, akik Személyi Biztonsági Tanúsítvánnyal rendelkeznek, a Szükséges Ismeret követelménye érvényesül velük kapcsolatban, valamint a Minősített Szerződéssel összefüggésben foglalkoztatják őket;
b) a Hatáskörrel Rendelkező Hatóságok által megállapított, a minősített adatok továbbítási rendjéhez szükséges intézkedések végrehajtása;
c) a Hatáskörrel Rendelkező Hatóság minősített adattal kapcsolatos esetleges változásokra vonatkozó értesítésére vonatkozó eljárások alkalmazása;
d) a Hatáskörrel Rendelkező Hatóságok által megállapított, az egyik Fél személyzetének a másiknál történő látogatására vonatkozó rendjének alkalmazása;
e) a Hatáskörrel Rendelkező Hatóság értesítése minden, a továbbított adattal kapcsolatos illetéktelen hozzáférésről, annak kísérletéről vagy gyanújáról;
f) az átvett minősített adat csak a Minősített Szerződés tárgyával összefüggésben használható fel;
g) a minősített adatok átadására, átvételére, feldolgozására és végleges megsemmisítésére vonatkozó eljárások a Felek hatályos jogszabályainak megfelelően történő alkalmazása.

6. A Minősített Szerződés végrehajtásába a Szerződő Fél alvállalkozót a Hatáskörrel Rendelkező Hatóság engedélyével vonhat be. Az alvállalkozónak ugyanazoknak a biztonsági feltételeknek kell eleget tennie, mint a Szerződő Félnek.

9. Cikk
A minősített adat továbbítása

1. A minősített adat továbbítása az Átadó Fél nemzeti jogszabályaiban meghatározott szabályok szerint, diplomáciai úton, vagy a Hatáskörrel Rendelkező Hatóságok megegyezése szerinti egyéb módon történik.

2. Az adat továbbításának a következő követelményeknek kell megfelelnie:

a) a futárnak az Átadó Fél, az Átvevő Fél vagy valamelyik Fél közigazgatásának az állandó alkalmazottjának kell lennie, és legalább olyan szintű Személyi Biztonsági Tanúsítvánnyal kell rendelkeznie, mint az átadandó adat;
b) a futárnak az alkalmazandó nemzeti jogszabályoknak megfelelő futárigazolvánnyal kell rendelkeznie;
c) a minősített adatot az Átadó Fél nemzeti jogszabályainak megfelelően be kell csomagolni és le kell zárni;
d) a minősített adat átvételét írásban haladéktalanul vissza kell igazolni.

3. Az átadott minősített adatot nyilvántartásba kell venni. A nyilvántartás kivonatát kérésre rendelkezésre kell bocsátani.

4. Amennyiben a minősített adat vagy anyag fenti szabályok szerinti továbbítása nem lehetséges, az érintett Hatáskörrel Rendelkező Hatóságok együttműködésével esetileg kell megszervezzék azt.

5. A Felek minősített adatot a Hatáskörrel Rendelkező Hatóságok által jóváhagyott eljárási rend szerint továbbíthatnak elektronikus úton.

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 Átadó Fél minősített adatát tartalmazza.

3. A minősített adatot sokszorosító vagy fordító személynek legalább olyan szintű Személyi Biztonsági Tanúsítvánnyal kell rendelkeznie, mint az átadott adat.

4. A Jelen Egyezmény alapján átadott, „TITKOS!” / SECRET DEFENSE minősítésű adat fordítása vagy sokszorosítása kizárólag az Átadó Fél előzetes írásbeli engedélyével lehetséges.

5. Főszabályként a jelen Egyezmény alapján átadott, „SZIGORÚAN TITKOS!” / TRES SECRET DEFENSE minősítésű adat fordítása vagy sokszorosítása nem megengedett, de az Átadó Fél Hatáskörrel Rendelkező Hatósága esetileg előzetes írásbeli eseti engedélyével jóváhagyhatja azt.

6. Jelen Egyezmény alapján átadott minősített adatot úgy kell megsemmisíteni, hogy teljes vagy részleges helyreállítása lehetetlenné váljon.

7. Jelen Egyezmény alapján átadott, „SZIGORÚAN TITKOS!” / TRES SECRET DEFENSE minősítésű adat nem semmisíthető meg, az ilyen minősítési szintű adatokat az Átadó Félnek kell visszaszolgáltatni.

8. A jelen Egyezmény alapján készített vagy átadott minősített adatot olyan válsághelyzet esetén, amely lehetetlenné teszi a minősítési szintjének és a jelen Egyezmény rendelkezéseinek megfelelő védelmét, ha visszajuttatása nem lehetséges, haladéktalanul meg kell semmisíteni. A megsemmisítésről az Átvevő Fél Nemzeti Biztonsági Felügyelete haladéktalanul értesíti az Átadó Fél Nemzeti Biztonsági Felügyeletét.

11. Cikk
Látogatások

1. Minősített adathoz való hozzáférést igénylő látogatásra a fogadó Fél Hatáskörrel Rendelkező Hatóságának előzetes írásbeli jóváhagyása alapján kerülhet sor.

2. A látogatásra vonatkozó megkeresést legalább 20 nappal a látogatás időpontja előtt a Hatáskörrel Rendelkező Hatósághoz kell benyújtani, amely azt továbbítja a fogadó Fél Hatáskörrel Rendelkező Hatóságához. Sürgős esetben a Hatáskörrel Rendelkező Hatóságok 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 létesítmény 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, fax száma, e-mail címe;
g) dátum, aláírás és a Hatáskörrel Rendelkező Hatóság hivatalos pecsétjének lenyomata.

4. A Hatáskörrel Rendelkező Hatóságok közösen meghatározhatják a visszatérő látogatásra jogosult személyek listáját. A visszatérő látogatások további részleteit a Hatáskörrel Rendelkező Hatóságok közösen állapítják meg.

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 Hatáskörrel Rendelkező Hatóságok késedelem nélkül írásban tájékoztatják egymást azon minősített adat biztonságának megsértéséről, amely esetben a jelen Egyezmény hatálya alá tartozó minősített adathoz való jogosulatlan hozzáférésre, a minősített adat jogosulatlan megváltoztatására vagy kezelésére kerül sor, vagy mindezek alapos gyanúja merül fel.

2. A Fél, amelyiknek területén a minősített adat biztonságának megsértésére sor került, nemzeti jogszabályainak megfelelően késedelem nélkül intézkedik a minősített adat megsértésének kivizsgálása érdekében. A másik Fél felkérés esetén részt vesz a vizsgálatban.

3. Az Átvevő Fél minden esetben írásban tájékoztatja az Átadó Felet a minősített adat biztonsága megsértésének körülményeiről, a kár mértékéről, a kár enyhítése érdekében megtett intézkedésekről, valamint a vizsgálat eredményéről. A tájékoztatásnak olyan részletesnek kell lennie, ami lehetővé teszi, hogy az Átadó Fél a minősített adat biztonsága megsértésének következményeit teljes körűen megítélhesse.

13. Cikk
Költségek viselése

1. Főszabályként jelen Egyezmény végrehajtása nem okozhat semmilyen külön költséget.

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

14. Cikk
Záró rendelkezések

1. Jelen Egyezmény határozatlan időre jön létre. Jelen Egyezmény a Felek az Egyezmény hatálybalépéséhez 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 hatálybalépésével 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 jogszolgáltatási fórum igénybevétele nélkül rendezik.

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

Készült Párizsban, 2012. december 11-én, két eredeti példányban, magyar és francia nyelven, mindkét szöveg egyaránt hiteles.

……. ……..

Magyarország Kormánya részéről

a Francia Köztársaság Kormánya részéről

ACCORD ENTRE LE GOUVERNEMENT DE LA HONGRIE ET LE GOUVERNEMENT DE LA REPUBLIQUE FRANÇAISE RELATIF A L'ECHANGE ET A LA PROTECTION RECIPROQUE DES INFORMATIONS CLASSIFIEES

Le Gouvernement de la Hongrie et le Gouvernement de la République française, ci-après dénommés « les Parties »,

Conscients du fait que la bonne marche de la coopération entre les Parties peut nécessiter l'échange d'informations classifiées,

Désireux de garantir la protection des informations et matériels classifiés échangés ou produits entre les deux Parties ou entre des personnes morales ou physiques placées sous leur juridiction,

Sont convenus de ce qui suit:

Article premier: Champ d'application

1. Le présent Accord régit l'échange de l'ensemble des informations classifiées transmises ou produites entre les Parties ou entre des personnes morales ou physiques placées sous leur juridiction.

2. Le présent Accord n'affecte pas les obligations qui découlent pour les Parties de tout autre traité bilatéral ou multilatéral, y compris tout accord régissant l'échange et la protection réciproque d'informations classifiées.

Article 2: Définitions

Aux fins du présent Accord :

a) l'expression « information classifiée » désigne toute information qui, quelle qu'en soit la forme ou la nature, requiert en vertu des lois et règlements nationaux de l'une ou l'autre des Parties une protection contre toute divulgation ou autre manipulation non autorisée et qui a été dûment désignée comme telle;

b) l'expression « contrat classifié » désigne un contrat qui renferme des informations classifiées ou nécessite l'accès à des informations classifiées;

c) le terme « contractant » désigne toute personne ayant la capacité juridique de négocier et de conclure un contrat classifié;

d) l'expression « Autorité nationale de sécurité » désigne l'autorité nationale chargée de la supervision et de la mise en œuvre du présent Accord pour chacune des Parties;

e) l'expression « Autorités compétentes » désigne toute Autorité, y compris toute Autorité de sécurité désignée ou toute autre entité compétente autorisée conformément aux lois et

règlements nationaux des Parties, chargée de la mise en œuvre du présent Accord en fonction du domaine concerné;

f) l'expression « Partie d'origine » désigne la Partie, y compris les personnes morales ou physiques relevant de sa juridiction, qui transmet des informations classifiées;

g) l'expression « Partie destinataire » désigne la Partie, y compris les personnes morales ou physiques relevant de sa juridiction, qui reçoit des informations classifiées;

h) l'expression « tierce partie » désigne tout État, y compris les personnes morales ou physiques relevant de sa juridiction, ou toute organisation internationale non partie au présent Accord;

i) l'expression « besoin d'en connaître » désigne le principe en vertu duquel l'accès à des informations classifiées ne peut être accordé qu'à une personne justifiant du besoin d'en avoir connaissance en rapport avec ses fonctions officielles dans le cadre desquelles ces informations ont été transmises à la Partie destinataire;

j) le terme « personne » désigne toute personne physique ou morale;

k) l'expression « habilitation de sécurité » désigne une décision positive découlant d'une procédure d'enquête et attestant la loyauté et la fiabilité d'une personne, de même que d'autres facteurs afférents à la sécurité, conformément aux lois et règlements nationaux des États des Parties. Cette décision permet à une personne d' avoir accès à des informations classifiées et l'autorise à les traiter ; les habilitations de sécurité délivrées à des personnes physiques sont dénommées « habilitations personnelles de sécurité », celles qui sont délivrées à des personnes morales sont dénommées « habilitations de sécurité d'établissement ».

Article 3: Autorités compétentes

1. Les Autorités nationales de sécurité des Parties chargées de la protection des informations classifiées ainsi que de la mise en œuvre du présent Accord sont:

Pour la Hongrie:
l'Autorité nationale de sécurité de Hongrie,
H-1024 Budapest, Szilágyi Erzsébet fasor 11/B.

Pour la République française:
le Secrétariat général de la Défense et de la Sécurité nationale (SGDSN),
51 boulevard de La Tour-Maubourg,
75700 Paris

2. Les Autorités nationales de sécurité s'informent mutuellement des coordonnées de leurs points de contact et de tout changement y afférent.

3. Les Parties s'informent mutuellement par la voie diplomatique de tout changement portant sur leur Autorité nationale de sécurité et sur les autres Autorités compétentes.

Article 4: Niveaux et mentions de classification de sécurité

1. L'équivalence des niveaux et mentions nationaux de classification de sécurité est définie ci-après:

En Hongrie	**En République française**
„SZIGORÚAN TITKOS!"	TRES SECRET DEFENSE
„TITKOS!"	SECRET DEFENSE
„BIZALMAS!"	CONFIDENTIEL DEFENSE
„KORLÁTOZOTT TERJESZTÉSŰ!"	DIFFUSION RESTREINTE

2. La République française traite et protège les informations portant la mention „KORLÁTOZOTT TERJESZTÉSŰ!", transmises par la Hongrie, conformément à ses lois et règlements nationaux en vigueur relatifs aux informations protégées mais non classifiées portant la mention « DIFFUSION RESTREINTE ».

3. La Hongrie traite et protège les informations non classifiées mais protégées par la mention « DIFFUSION RESTREINTE », transmises par la République française, conformément à ses lois et règlements nationaux en vigueur relatifs à la protection des informations portant la mention „KORLÁTOZOTT TERJESZTÉSŰ!".

4. Lorsque, pour des raisons particulières de sécurité, la Partie d'origine demande que l'accès à des informations classifiées soit limité à des personnes possédant uniquement la nationalité des Parties, ces informations doivent porter la mention complémentaire « SPECIAL FRANCE-HONGRIE » ou « SPECIAL HONGRIE-FRANCE ».

Article 5: Accès aux informations classifiées

L'accès aux informations classifiées de niveau „BIZALMAS!" / CONFIDENTIEL DEFENSE ou supérieur en vertu du présent Accord est réservé uniquement aux personnes physiques justifiant du besoin d'en connaître et habilitées au niveau requis conformément aux lois et règlements nationaux de la Partie considérée.

Article 6: Principes de sécurité

1. La Partie d'origine :

a) veille à ce que les informations classifiées portent la mention de classification de sécurité appropriée conformément à ses lois et règlements nationaux;
b) informe la Partie destinataire de toute restriction éventuelle à l'utilisation d'informations classifiées;
c) informe la Partie destinataire sans retard de tout changement ultérieur du niveau de classification de sécurité de toute information classifiée échangée.

2. La Partie destinataire :

a) appose sa propre mention de classification sur les informations classifiées reçues de la Partie d'origine, conformément aux équivalences définies à l'article 4;

b) leur accorde le même degré de protection qu'à ses propres informations classifiées de niveau équivalent;
c) veille à ce qu'elles ne soient pas déclassifiées ni ne fassent l'objet d'un changement de niveau de classification sans l'accord écrit préalable de la Partie d'origine;
d) veille à ce qu'elles ne soient pas divulguées à une tierce partie sans l'accord écrit préalable de la Partie d'origine;
e) ne les utilise qu'aux fins pour lesquelles elles ont été transmises et conformément aux conditions de divulgation définies par la Partie d'origine.

3. Aux fins du traitement et du contrôle des informations classifiées dans chacun des organismes (institutions, sociétés) des Parties qui crée, remanie et/ou détient des informations classifiées, il est mis en place un système d'enregistrement couvrant la réception, la diffusion, le contrôle et la protection des informations classifiées. Ce système doit avoir été accrédité par une autorité compétente de l'État considéré.

4. Tout système de communication et d'information utilisé pour le traitement des informations classifiées échangées sous forme électronique en vertu du présent Accord doit avoir été accrédité par l'autorité compétente de l'État considéré.

Article 7: Coopération en matière de sécurité

1. Afin de maintenir des normes de sécurité comparables, les Autorités compétentes s'informent mutuellement, à leur demande, de leurs lois et règlements nationaux relatifs à la protection des informations classifiées et des pratiques qui découlent de leur application. Elles s'informent mutuellement de toute modification de fond afférente à l'Accord.

2. Les Autorités compétentes peuvent, à leur demande et conformément à leurs lois et règlements nationaux, se prêter assistance au cours des procédures d'habilitation personnelle de sécurité et d'habilitation de sécurité d'établissement.

3. Les Parties reconnaissent, à leur demande et conformément à leurs lois et règlements nationaux, les habilitations personnelles de sécurité et les habilitations de sécurité d'établissement délivrées par l'autre Partie.

4. En cas de retrait ou de déclassement d'habilitations personnelles de sécurité ou d'habilitations de sécurité d'établissement reconnues, les Autorités compétentes s'en informent promptement.

Article 8: Contrats classifiés

1. Les contrats classifiés doivent être conclus et exécutés conformément aux lois et règlements nationaux de chaque Partie. Les Autorités compétentes attestent, sur demande, que les contractants envisagés et les personnes physiques qui prennent part à la négociation préalable ou à l'exécution de contrats classifiés disposent de l'habilitation personnelle de sécurité ou de l'habilitation de sécurité d'établissement appropriée.

2. L'Autorité compétente peut demander à son homologue qu'il soit procédé à une visite de sécurité d'une installation située sur le territoire de l'autre Partie afin d'assurer la protection constante des informations classifiées.

3. L'Autorité compétente de la Partie sur le territoire de laquelle le contrat doit être exécuté veille à ce que soit appliqué et maintenu, dans le cadre de la mise en œuvre de contrats classifiés, un niveau de sécurité équivalent au niveau requis pour assurer la protection de ses propres contrats classifiés.

4. Les contrats classifiés doivent comprendre des instructions de sécurité ainsi qu'un guide de classification. Ces instructions, conformes à celles de l'Autorité compétente de la Partie d'origine, précisent les informations qui doivent être protégées par la Partie destinataire et le niveau de classification approprié. Un exemplaire des instructions de sécurité du projet et du guide de classification est transmis à l'Autorité compétente de la Partie dont relève l'exécution du contrat classifié.

5. Les obligations du contractant en matière de protection des informations classifiées sont au minimum les suivantes:

a) ne divulguer d'informations classifiées qu'à des personnes qui détiennent une habilitation de sécurité, qui justifient du besoin d'en connaître et qui sont employées dans le cadre des contrats;
b) mettre en œuvre les moyens nécessaires pour assurer la transmission d'informations classifiés, comme établi par les Autorités compétentes;
c) mettre en œuvre les procédures et mécanismes permettant d'informer son Autorité compétente de tout changement susceptible de survenir à l'égard d'informations classifiées;
d) mettre en œuvre les procédures de visites de personnel d'une Partie à l'autre Partie, telles qu'établies par les Autorités compétentes;
e) informer son Autorité compétente de tout fait avéré, tentative ou soupçon d'accès non autorisé aux informations classifiées échangées;
f) n'utiliser les informations classifiées qu'il reçoit qu'aux fins en rapport avec l'objet du contrat classifié;
g) se conformer aux procédures établies par les lois et règlements respectifs en vigueur dans les États des Parties en ce qui concerne la réception, la transmission, le traitement et la destruction finale d'informations classifiées.

6. Avant d'exécuter un contrat classifié avec un sous-traitant, le contractant doit y avoir été autorisé par ses Autorités compétentes. Les sous-traitants doivent se conformer aux mêmes conditions de sécurité que le contractant.

Article 9: Transmission des informations classifiées

1. Les informations classifiées sont transmises conformément aux lois et règlements nationaux de la Partie d'origine par la voie diplomatique ou selon toutes autres modalités convenues entre les Autorités compétentes.

2. La transmission doit satisfaire aux conditions suivantes:

a) le courrier est employé en permanence par la Partie d'origine, par la Partie destinataire ou par l'administration d'une des Parties et est habilité à un niveau au moins égal à celui des informations classifiées à transmettre;
b) le courrier détient une lettre de courrier délivrée conformément aux lois et règlements nationaux applicables;
c) les informations classifiées sont dûment empaquetées et scellées conformément aux lois et règlements nationaux de la Partie d'origine ;
d) la réception des informations classifiées est confirmée par écrit sans retard.

3. Les informations classifiées transmises doivent avoir été enregistrées. Une copie du registre est fournie sur demande.

4. La transmission d'informations ou de matériels classifiés qui ne peut s'opérer conformément aux règles énoncées ci-dessus est organisée au cas par cas entre les Autorités compétentes respectives.

5. Les Parties peuvent transmettre des informations classifiées par des moyens électroniques conformément aux procédures de sécurité approuvées par les Autorités compétentes.

Article 10: Reproduction, traduction et destruction d'informations classifiées

1. Les reproductions et traductions d'informations classifiées transmises en vertu du présent Accord portent les mêmes mentions de classification de sécurité que les originaux et sont protégées de la même manière que ceux-ci. Le nombre des reproductions est limité au nombre requis à des fins officielles.

2. Les traductions d'informations classifiées transmises en vertu du présent Accord doivent comporter une note rédigée dans la même langue et précisant qu'elles renferment des informations classifiées de la Partie d'origine.

3. La traduction et la reproduction d'informations classifiées ne peuvent être assurées que par des personnes habilitées au moins au même niveau que celui des documents considérés.

4. Les informations classifiées transmises en vertu du présent Accord et portant la mention „TITKOS!" / SECRET DEFENSE ne peuvent être traduites ou reproduites qu'avec l'accord écrit préalable de la Partie d'origine.

5. Les informations classifiées transmises en vertu du présent Accord et portant la mention „SZIGORÚAN TITKOS!" / TRES SECRET DEFENSE ne peuvent en principe être ni traduites ni reproduites; l'Autorité compétente d'origine peut toutefois l'autoriser au cas par cas par accord écrit préalable.

6. Les informations classifiées transmises en vertu du présent Accord sont détruites de telle manière que leur reconstitution totale ou partielle soit impossible.

7. Les informations classifiées transmises en vertu du présent Accord et portant la mention „SZIGORÚAN TITKOS!" / TRES SECRET DEFENSE ne doivent pas être détruites mais restituées à la Partie d'origine.

8. En situation de crise rendant impossible la protection, conformément à leur mention de classification et aux dispositions du présent Accord d'informations classifiées produites ou transmises en vertu du présent Accord, et si leur restitution n'est pas possible, celles-ci doivent être détruites aussitôt. L'Autorité nationale de sécurité de la Partie destinataire informe de leur destruction l'autorité nationale de sécurité de la Partie d'origine dès que possible.

Article 11: Visites

1. Les visites qui nécessitent l'accès à des informations classifiées sont soumises à l'accord écrit préalable de l'Autorité compétente de la Partie d'accueil.

2. Les demandes de visite sont présentées au moins vingt jours à l'avance à l'Autorité compétente, laquelle les transmet à l'Autorité compétente de la Partie d'accueil. En cas d'urgence, une demande de visite peut être présentée dans un délai plus bref, sous réserve de coordination préalable entre les Autorités compétentes.

3. Les demandes de visite doivent comporter:

a) l'identité, la date et le lieu de naissance, la nationalité et le numéro de passeport ou de carte d'identité du visiteur;
b) la fonction du visiteur et le nom de la personne morale qu'il représente;
c) le niveau de l'habilitation personnelle de sécurité du visiteur et sa validité;
d) la date et la durée de la visite ou, en cas de visites multiples, la période couverte par celles-ci;
e) l'objet de la visite, y compris le niveau de classification le plus élevé des informations classifiées mises en jeu;
f) le nom et l'adresse de l'installation qui fait l'objet de la visite, ainsi que le nom, les numéros de téléphone et de télécopie et l'adresse électronique de son point de contact;
g) la date, la signature et le timbre officiel de l'Autorité compétente.

4. Les Autorités compétentes peuvent établir d'un commun accord une liste de personnes autorisées à effectuer plusieurs visites. Elles conviennent des autres modalités applicables à ces visites.

5. Les informations classifiées dont un visiteur a connaissance sont considérées comme des informations classifiées reçues en vertu du présent Accord.

Article 12: Atteinte à la sécurité

1. Les Autorités compétentes s'informent mutuellement par écrit et sans retard de toute atteinte à la sécurité qui a eu pour effet la divulgation non autorisée d'informations classifiées relevant du présent Accord ou toute autre manipulation non autorisée desdites informations, ainsi que de tout soupçon fondé en la matière.

2. La Partie sur le territoire de laquelle cette atteinte à la sécurité s'est produite diligente aussitôt une enquête conformément à ses lois et règlements nationaux. L'autre Partie coopère à l'enquête sur demande.
3. La Partie destinataire informe dans tous les cas la Partie d'origine, par écrit, des circonstances dans lesquelles l'atteinte à la sécurité s'est produite, de l'étendue des

dommages, des mesures prises pour y remédier et des résultats de l'enquête. Ces informations doivent permettre à la Partie d'origine d'évaluer pleinement les conséquences de cette atteinte à la sécurité.

Article 13: Frais

1. La mise en œuvre du présent Accord n'engendre pas, en principe, de frais spécifiques.

2. Chaque Partie contractante prend en charge les frais encourus par elle dans le cadre de l'application du présent Accord.

Article 14: Dispositions finales

1. Le présent Accord est conclu pour une durée indéterminée. Il entrera en vigueur le premier jour du deuxième mois suivant la réception de la dernière des notifications échangées entre les Parties par la voie diplomatique et attestant l'accomplissement des procédures légales internes requises pour son entrée en vigueur.

2. Le présent Accord peut être modifié d'un commun accord des Parties établi par écrit. Les modifications entrent en vigueur conformément au paragraphe 1.

3. Chaque Partie peut à tout moment dénoncer le présent Accord par écrit. Dans ce cas, il parviendra à expiration après un délai de six mois à compter de la date à laquelle l'autre Partie aura reçu notification écrite de sa dénonciation.

4. Nonobstant la dénonciation du présent Accord, les informations classifiées échangées ou produites en vertu de celui-ci seront protégées conformément aux dispositions ci-dessus jusqu'à ce que la Partie d'origine ait dispensé par écrit la Partie destinataire de cette obligation.

5. Tout différend relatif à l'interprétation ou à l'application du présent Accord est réglé par voie de consultations et de négociations entre les Parties, sans recours à une juridiction extérieure.

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

Fait à PARIS le 11 décembre 2012 le en deux exemplaires originaux en langues hongroise et française, les deux textes faisant également foi

Pour le Gouvernement de la Hongrie

Pour le Gouvernement
de la République française"

4. §

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

(2) A 2. § és 3. § az Egyezmény 14. Cikk 1. pontjában meghatározott időpontban lép hatályba.

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

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

INDOKOLÁS A MAGYARORSZÁG KORMÁNYA ÉS A FRANCIA KÖZTÁRSASÁG KORMÁNYA KÖZÖTT A MINŐSÍTETT ADATOK CSERÉJÉRŐL ÉS KÖLCSÖNÖS VÉDELMÉRŐL SZÓLÓ EGYEZMÉNY KIHIRDETÉSÉRŐL SZÓLÓ TÖRVÉNYJAVASLATHOZ

ÁLTALÁNOS INDOKOLÁS

Az Országgyűlés 2009. december 14-én fogadta el a minősített adat védelméről szóló 2009. évi CLV. törvényt (a továbbiakban: Mavtv.), amely az államtitokról és a szolgálati titokról szóló 1995. évi LXV. törvény, valamint a Nemzeti Biztonsági Felügyeletről szóló 1998. évi LXXXV. törvény helyébe lépett. A 2010. április 1-jétől hatályos új jogszabály alapjaiban kodifikálta újra a minősített adatok védelmének magyarországi struktúráját. Megteremtette a minősített adatok védelmének egységes jogszabály- és intézményrendszerét, s egyúttal eleget tett legfontosabb jogharmonizációs kötelezettségeinknek. A minősített adat védelméről szóló új törvény megalkotását indokolta az államtitokról és a szolgálati titokról szóló 1995. évi LXV. törvény átfogó felülvizsgálatának szükségessége: hiányoztak a külföldi (NATO, EU) és a nemzeti minősített adatok védelmére [elektronikus biztonságra (INFOSEC)] vonatkozó szabályok, az EU csatlakozásunk óta módosított EU normák átvételére, valamint az ehhez szükséges jogintézmények (a nemzeti személyi és telephely biztonsági tanúsítványok, nemzeti iparbiztonsági rendszer) bevezetésére nem került sor.

A minősített adatok cseréjére vonatkozó biztonsági együttműködés érdekében – a katonai megállapodások kivételével – hazánk jogszabályi felhatalmazás hiányában korábban csak két állammal kötött általános titokvédelmi egyezményt (*a Magyar Köztársaság Kormánya és az Olasz Köztársaság Kormánya között a minősített információk védelméről szóló, Budapesten, 2003. március 20-án aláírt Biztonsági Megállapodás kihirdetéséről szóló 2004. évi LXXXIX. törvény, valamint a Magyar Köztársaság Kormánya és a Németországi Szövetségi Köztársaság Kormánya között a minősített információk kölcsönös védelme tárgyában Budapesten, 1995. október 25-én aláírt Egyezmény megerősítéséről és kihirdetéséről szóló 1996. évi XXXV. törvény),* amelyek alkalmazását a 2010. március 31-ig hatályos, az államtitokról és szolgálati titokról szóló 1995. évi LXV. törvény nem tette lehetővé.

A minősített adat védelméről szóló 2009. évi CLV. törvény 2010. április 1-jei hatálybalépésével azonban megteremtette a kétoldalú titokvédelmi megállapodások megkötéséhez és alkalmazásához szükséges jogi alapokat, és így megkezdődhetett hazánk e téren tapasztalható elmaradásának felszámolása. Ennek megfelelően hazánk először a 46/2011. (VI. 21.) ME határozat értelmében a Szlovák Köztársasággal, a Lengyel Köztársasággal és a Cseh Köztársasággal kezdte meg a tárgyalásokat, melyek közül 2012. május 3-án aláírásra került Budapesten a Szlovák Köztársaság és Magyarország, 2012. június 13-án a Cseh Köztársaság és Magyarország, 2012. augusztus 29-én pedig már az 58/2012. (V.16) ME határozat alapján a Lett Köztársaság és Magyarország között a minősített adatok cseréjéről és kölcsönös védelméről szóló egyezmény.

A Mavtv-ben foglaltak végrehajtása, Magyarország nemzetközi kötelezettségvállalásainak teljesítése, továbbá a minősített adatok cseréjével és kölcsönös védelmével történő szorosabb együttműködés biztosítása miatt azonban indokolt új szerződések megkötése.

RÉSZLETES INDOKOLÁS

Az 1. §-hoz

A Javaslat 1. §-a a nemzetközi szerződésekkel kapcsolatos eljárásról szóló 2005. évi L. törvény 7. § (1)-(3) bekezdésének, valamint 10. § (1) bekezdés *a)* pontjának megfelelően tartalmazza az Egyezmény kötelező hatályának elismerésére adott országgyűlési felhatalmazást.

A 2. és 3. §-hoz

A Javaslat 2. §-a és 3. §-a a nemzetközi szerződésekkel kapcsolatos eljárásról szóló 2005. évi L. törvény 10. § (1) bekezdés *b)* pontjának megfelelően rendelkezik az Egyezmény kihirdetéséről, és tartalmazza az Egyezmény francia és magyar nyelvű hiteles szövegét.

Az Egyezmény célja, hogy védelmet biztosítson a Szerződő Felek, valamint a joghatóságuk alá tartozó jogi személyek és természetes személyek közötti együttműködés során kicserélt vagy keletkezett minősített adatok számára. Ennek keretében szabályozza a Felek közötti biztonsági együttműködést, kijelöli a hatáskörrel rendelkező hatóságokat, és rendelkezik

egyes nemzeti minősítési szintek egymásnak történő megfeleltethetőségéről, valamint a minősített adat biztonságának megsértése esetén alkalmazandó eljárásról.

A 4. §-hoz

A Javaslat a kihirdetését követő napon lép hatályba. Az Egyezmény 14. Cikk 1. pontja szerint a „*Jelen Egyezmény a Felek az Egyezmény hatálybalépéséhez szükséges belső feltételek teljesítésére vonatkozó, diplomáciai úton küldött utolsó értesítése kézhezvételének napját követő második hónap első napján lép hatályba.”*. Ennek oka, hogy az Egyezmény kötelező hatályának elismerésére a Felek által alkalmazandó alkotmányos vagy belső jogi szabályokkal és eljárásokkal összhangban kerüljön sor. Az Egyezmény hatálybalépésének naptári napját a külpolitikáért felelős miniszter annak ismertté válását követően a Magyar Közlönyben közzétett egyedi közleményével állapítja meg.