MAGYARORSZÁG KORMÁNYA

Átiktatva: T/407.

~~**T/20373. számú**~~

törvényjavaslat

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

Előadó: Dr. Pintér Sándor
belügyminiszter

Budapest, 2018. március

2018. évi … törvény

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

1. §

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

2. §

Az Országgyűlés az Egyezményt e törvénnyel kihirdeti.

3. §

Az Egyezmény hiteles magyar és angol nyelvű szövege a következő:

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

Magyarország Kormánya és a Finn Köztársaság Kormánya (a továbbiakban: „Felek”)

annak érdekében, hogy védelemben részesítsék a minősített adatokat, különösen amelyek a külügyi kapcsolatok, a védelem, a biztonság, rendőrségi vagy tudományos, ipari és technológiai együttműködési területek vonatkozásában kerültek közvetlen átadásra a Felek között vagy azon jogi személyek vagy természetes személyek között, amelyek, illetve akik a Felek joghatósága alatt minősített adatot kezelnek,

az alábbiakban állapodtak meg:

1. CIKK
AZ EGYEZMÉNY CÉLJA ÉS HATÁLYA

Jelen Egyezmény célja a Felek közötti együttműködési folyamat során kicserélt vagy keletkezett minősített adatok védelmének biztosítása.

2. CIKK
FOGALOMMEGHATÁROZÁSOK

Jelen Egyezmény alkalmazásában:

a) *minősített adat*: megjelenési formájától, természetétől vagy a Felek által alkalmazott átadás módjától függetlenül minden olyan adat, okirat vagy anyag, amelyet minősítettek és a nemzeti jogszabályokkal és egyéb szabályokkal összhangban megfelelő minősítési jelöléssel láttak el, továbbá az olyan adat, okirat vagy anyag, amelyet ilyen minősített adat alapján hoztak létre és megfelelő jelöléssel láttak el;
b) *minősített szerződés*: olyan szerződés vagy alvállalkozói szerződés, amely minősített adatot tartalmaz vagy foglal magában;
c) *szerződő*: olyan jogi személy vagy természetes személy, aki a nemzeti jogszabályokkal és egyéb szabályokkal összhangban rendelkezik a minősített szerződések megkötésére irányuló képességgel;
d) *átadó Fél:* az a Fél, amelyik a minősített adatot átadja, vagy amelynek fennhatósága alatt minősített adat keletkezett;
e) *átvevő Fél:* az a Fél – beleértve a joghatósága alá tartozó jogi személyeket vagy természetes személyeket –, amelynek az átadó Fél a minősített adatot átadja;
f) *hatáskörrel rendelkező biztonsági hatóság*: az a nemzeti biztonsági hatóság, kijelölt biztonsági hatóság vagy egyéb, hatáskörrel rendelkező, a Felek nemzeti jogszabályaival és egyéb szabályaival összhangban felhatalmazott szervezet, amely jelen Egyezmény végrehajtásáért felelős;
g) *a minősített adat biztonságának megsértése*: olyan cselekmény vagy mulasztás, amely a nemzeti jogszabályokkal és egyéb szabályokkal ellentétes, és amely a minősített adat elvesztését vagy megsértését eredményezheti;
h) *biztonsági tanúsítvány:* nemzetbiztonsági ellenőrzés eredményeként született azon pozitív döntés, amelyben megállapításra kerül, hogy egy jogi személy (*telephely biztonsági tanúsítvány*, TBT) vagy egy természetes személy (*személyi biztonsági tanúsítvány*, SZBT) a nemzeti jogszabályokkal és egyéb szabályokkal összhangban alkalmas az adott minősítési szintű minősített adathoz való hozzáférésre és a minősített adat kezelésére;
i) *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
HATÁSKÖRREL RENDELKEZŐ BIZTONSÁGI HATÓSÁGOK

(1) A jelen Egyezmény általános végrehajtásáért felelős, a Felek által kijelölt nemzeti biztonsági hatóságok (NSA):

Magyarországon:	**A Finn Köztársaságban:**

Nemzeti Biztonsági Felügyelet (NBF)	Külügyminisztérium Ulkoasiainministeriö Nemzeti Biztonsági Felügyelet Kansallinen turvallisuusviranomainen

(2) A Felek tájékoztatják egymást minden olyan hatáskörrel rendelkező biztonsági hatóságról, amely jelen Egyezmény egyes részeinek végrehajtásáért felelős.
(3) A Felek tájékoztatják egymást a hatáskörrel rendelkező biztonsági hatóságokkal kapcsolatos későbbi változásokról.

4. CIKK
MINŐSÍTÉSI SZINTEK

(1) A jelen Egyezmény alapján átadott minősített adatokat a Felek nemzeti jogszabályaival és egyéb szabályaival összhangban a megfelelő minősítési szint szerinti jelöléssel kell ellátni.
(2) Az egyes minősítési szintek az alábbiak szerint feleltethetők meg egymásnak:

Magyarországon	**A Finn Köztársaságban**	**Angol megfelelőjük**
„Szigorúan titkos!”	ERITTÄIN SALAINEN vagy YTTERST HEMLIG	TOP SECRET
„Titkos!”	SALAINEN vagy HEMLIG	SECRET
„Bizalmas!”	LUOTTAMUKSELLINEN vagy KONFIDENTIELL	CONFIDENTIAL
„Korlátozott terjesztésű!”	KÄYTTÖ RAJOITETTU vagy BEGRÄNSAD TILLGÅNG	RESTRICTED

(3) Az átvevő Fél biztosítja, hogy a minősítés nem kerül megváltoztatásra vagy visszavonásra, az átadó Fél előzetes írásbeli engedélye nélkül.-

5. CIKK
MINŐSÍTETT ADATOK VÉDELME

(1) A Felek nemzeti jogszabályaikkal és egyéb szabályaikkal összhangban minden megfelelő intézkedést megtesznek az Egyezmény hatálya alá tartozó minősített adatok védelme

érdekében. Ezeket az adatokat ugyanolyan szintű védelemben részesítik, mint amelyet a saját, azonos minősítési szintű adataik számára biztosítanak.
(2) A Felek biztosítják, hogy az átadó Fél előzetes írásbeli hozzájárulása nélkül minősített adatot harmadik fél részére nem adnak át.
(3) Minősített adathoz való hozzáférést kizárólag olyan természetes személyek kaphatnak, akik a szükséges ismeret elvének megfelelnek, és akikre vonatkozóan a nemzeti jogszabályokkal és egyéb szabályokkal összhangban nemzetbiztonsági ellenőrzés került lefolytatásra, és akik felhatalmazást kaptak az ezen adatokhoz való hozzáférésre, valamint tájékoztatásban részesültek a minősített adatok védelmével kapcsolatos kötelezettségeikről.
(4) „Korlátozott terjesztésű!" vagy KÄYTTÖ RAJOITETTU / BEGRÄNSAD TILLGÅNG minősítésű adathoz való hozzáféréshez nincs szükség személyi biztonsági tanúsítványra.
(5) Minősített adat kizárólag az átadás során megjelölt célra használható fel.

6. CIKK
MINŐSÍTETT SZERZŐDÉSEK

(1) Az átvevő Fél hatáskörrel rendelkező biztonsági hatósága megkeresésre tájékoztatja az átadó Fél hatáskörrel rendelkező biztonsági hatóságát arról, hogy a szerződéskötést megelőző tárgyalásokban vagy a minősített szerződések teljesítésében részt vevő, javasolt szerződők rendelkeznek-e az adott minősítési szinthez szükséges szintű biztonsági tanúsítvánnyal. Ha a szerződő nem rendelkezik biztonsági tanúsítvánnyal, az átadó Fél hatáskörrel rendelkező biztonsági hatósága kérelmezheti, hogy az átvevő Fél hatáskörrel rendelkező biztonsági hatósága intézkedjen a szerződő nemzetbiztonsági ellenőrzésének lefolytatásáról.
(2) Nyílt pályázat esetén az átvevő Fél hatáskörrel rendelkező biztonsági hatósága hivatalos megkeresés nélkül is átadhatja az átadó Fél biztonsági hatósága részére a vonatkozó biztonsági tanúsítványokat.
(3) „Korlátozott terjesztésű!" vagy KÄYTTÖ RAJOITETTU / BEGRÄNSAD TILLGÅNG minősítési szint esetén telephely biztonsági tanúsítvány kibocsátása nem szükséges.
(4) A megfelelő biztonsági felügyelet és ellenőrzés biztosítása érdekében a minősített szerződésnek tartalmaznia kell az 1. melléklet szerinti biztonsági előírásokat, ideértve a minősítésekre vonatkozó útmutatót is. A biztonsági előírások másolata továbbításra kerül azon Fél hatáskörrel rendelkező biztonsági hatósága részére, melynek joghatósága alatt a szerződés teljesítésre kerül.
(5) A Felek hatáskörrel rendelkező biztonsági hatóságainak képviselői látogatást tehetnek a másik Félnél a szerződő által a minősített szerződésben foglalt minősített adatok védelme érdekében hozott előírások hatékonyságának ellenőrzése érdekében.

7. CIKK
MINŐSÍTETT ADATOK TOVÁBBÍTÁSA

(1) A minősített adat Felek közötti továbbítása biztosított kormányközi csatornákon vagy a hatáskörrel rendelkező biztonsági hatóságok által meghatározott egyéb módon történik.
(2) Minősített adatot a Felek egymás között elektronikusan kizárólag a hatáskörrel rendelkező biztonsági hatóságok kölcsönös megállapodása szerinti, biztonságos úton továbbítanak.

8. CIKK

MINŐSÍTETT ADATOK SOKSZOROSÍTÁSA, FORDÍTÁSA ÉS MEGSEMMISÍTÉSE

(1) A minősített adatról készült sokszorosított példányokon – beleértve a kivonatokat is – és fordításokon fel kell tüntetni a megfelelő minősítési szintet, és az így készült adatot ugyanolyan védelemben kell részesíteni, mint az eredeti minősített adatot. A sokszorosított és lefordított példányok számát a hivatalos célból szükséges minimumra kell korlátozni.
(2) Minden fordítás részét képezi egy, a fordítás nyelvén készült, megfelelő jelzés, amelyben feltüntetésre kerül, hogy az az átadó Fél minősített adatát tartalmazza.
(3) „Szigorúan titkos!” vagy ERITTÄIN SALAINEN / YTTERST HEMLIG vagy a 4. cikk szerint annak megfelelő minősítési szintű adat sokszorosítása vagy fordítása kizárólag az átadó Fél előzetes írásbeli hozzájárulásával történhet.
(4) „Szigorúan titkos!” vagy ERITTÄIN SALAINEN / YTTERST HEMLIG vagy a 4. cikk szerint annak megfelelő minősítési szintű adat nem semmisíthető meg az átadó Fél előzetes írásbeli engedélye nélkül. Az ilyen adatot az átadó Fél részére kell visszaküldeni, ha a Feleknek már nincs szükségük rá.
(5) A „Titkos!” vagy SALAINEN / HEMLIG vagy a 4. cikk szerint annak megfelelő vagy alacsonyabb minősítési szintű minősített adatot a nemzeti jogszabályokkal és egyéb szabályokkal összhangban meg kell semmisíteni, ha az átvevő Félnek már nincs szüksége rá.
(6) Olyan válsághelyzet esetén, amely lehetetlenné teszi a jelen Egyezmény alapján átadott minősített adat védelmét, a minősített adatot haladéktalanul meg kell semmisíteni. A minősített adat megsemmisítésről az átvevő Fél haladéktalanul értesíti az átadó Fél hatáskörrel rendelkező biztonsági hatóságát.

9. CIKK

LÁTOGATÁSOK

(1) „Bizalmas!” vagy LUOTTAMUKSELLINEN / KONFIDENTIELL vagy magasabb minősítési szintű minősített adathoz való hozzáférést igénylő látogatásra a fogadó Fél hatáskörrel rendelkező biztonsági hatóságának előzetes írásbeli hozzájárulása alapján kerülhet sor. A látogatók csak akkor kaphatnak hozzáférést, ha:

a) a küldő Fél hatáskörrel rendelkező biztonsági hatósága felhatalmazást adott a kért látogatás vagy látogatások lebonyolítására,
b) rendelkeznek a megfelelő személyi biztonsági tanúsítvánnyal, valamint
c) felhatalmazást kaptak minősített adatok átvételére a fogadó Fél nemzeti jogszabályaival és egyéb szabályaival összhangban.

(2) A kérelmet benyújtó Fél hatáskörrel rendelkező, érintett biztonsági hatósága a fogadó Fél hatáskörrel rendelkező, érintett biztonsági hatóságát a tervezett látogatásról jelen cikk rendelkezéseivel összhangban tájékoztatja és biztosítja, hogy a kérelmet a fogadó Fél legalább 14 nappal a látogatás időpontja előtt megkapja. Sürgős esetben a hatáskörrel rendelkező biztonsági hatóságok rövidebb határidőben is megállapodhatnak. A látogatási kérelemnek tartalmaznia kell a jelen Egyezmény 2. mellékletében meghatározott információkat.

(3) Az ismétlődő látogatásokra szóló engedély 12 hónapnál hosszabb időtartamra nem szólhat.

10. CIKK
BIZTONSÁGI EGYÜTTMŰKÖDÉS

(1) Jelen Egyezmény végrehajtása érdekében a nemzeti biztonsági hatóságok tájékoztatják egymást a minősített adatok védelmével kapcsolatos nemzeti jogszabályaikról és egyéb szabályaikról, valamint mindezek későbbi módosításáról.
(2) A jelen Egyezmény végrehajtásához szükséges szoros együttműködés biztosítása érdekében a hatáskörrel rendelkező biztonsági hatóságok egyeztetnek egymással. Megkeresés esetén a Felek tájékoztatják egymást a minősített adatok védelmére vonatkozó nemzeti biztonsági előírásaikról, eljárásaikról és gyakorlataikról. Ennek érdekében a hatáskörrel rendelkező biztonsági hatóságok látogatásokat tehetnek egymásnál.
(3) Megkeresés esetén a hatáskörrel rendelkező biztonsági hatóságok a nemzeti jogszabályokkal és egyéb szabályokkal összhangban segítséget nyújtanak egymásnak a biztonsági tanúsítványokkal kapcsolatos eljárások során.
(4) A nemzeti biztonsági hatóságok haladéktalanul értesítik egymást az érintett biztonsági tanúsítványokkal kapcsolatos változásokról.

11. CIKK
A MINŐSÍTETT ADAT BIZTONSÁGÁNAK MEGSÉRTÉSE

(1) A Felek haladéktalanul tájékoztatják egymást a minősített adat biztonságának bármilyen megsértéséről vagy annak gyanújáról.
(2) A joghatósággal rendelkező Fél késedelem nélkül kivizsgálja az eseményt. A másik Fél igény esetén együttműködik a vizsgálatban.
(3) A joghatósággal rendelkező Fél a nemzeti jogszabályokkal és egyéb szabályokkal összhangban megtesz minden lehetséges megfelelő intézkedést a jelen cikk (1) bekezdésében meghatározott esemény következményeinek enyhítése és a minősített adat biztonsága ismételt megsértésének megelőzése érdekében. A másik Felet a vizsgálat eredményéről és a megtett intézkedésekről tájékoztatni szükséges.

12. CIKK
KÖLTSÉGVISELÉS

A Felek maguk viselik a jelen Egyezménnyel kapcsolatos kötelezettségeik teljesítése során felmerült költségeiket.

13. CIKK
VITÁK RENDEZÉSE

A jelen Egyezmény értelmezéséből vagy alkalmazásából fakadó vitákat a Felek kizárólag egymás közötti egyeztetés útján rendezik.

14. CIKK
MÁS NEMZETKÖZI EGYEZMÉNYEKHEZ VALÓ VISZONY

Jelen Egyezmény nem érinti a Felek egyéb két- vagy többoldalú szerződések alapján fennálló kötelezettségeit, ideértve mindazon megállapodásokat, amelyek minősített adatok cseréjét és kölcsönös védelmét szabályozzák.

15. CIKK
ZÁRÓ RENDELKEZÉSEK

(1) A Felek tájékoztatják egymást a jelen Egyezmény hatálybalépéséhez szükséges nemzeti intézkedéseik teljesítéséről. Jelen Egyezmény az erről szóló későbbi értesítés kézhezvételét követő második hónap első napján lép hatályba.
(2) Jelen Egyezmény visszavonásig hatályban marad. Az Egyezmény a Felek kölcsönös egyetértésével írásban módosítható. Módosítás bármelyik Fél által bármikor kezdeményezhető. Amennyiben valamelyik Fél ilyen kezdeményezést tesz, a Felek az Egyezmény módosításával kapcsolatban egyeztetésbe kezdenek.
(3) Bármelyik Fél jogosult jelen Egyezményt felmondani a másik Félnek diplomáciai úton küldött írásbeli értesítéssel, 6 hónapos felmondási idővel. Felmondás esetén a már átadott és jelen Egyezmény hatálya alatt keletkezett minősített adatokat az Egyezmény rendelkezéseivel összhangban kell kezelni mindaddig, amíg a minősített adat védelméhez erre szükség van.
(4) Jelen Egyezmény hatálybalépését követően azon Fél, amelynek területén az Egyezmény aláírása történik, haladéktalanul intézkedik arról, hogy az Egyezményt az Egyesült Nemzetek Szervezetének Titkársága regisztrálja az Egyesült Nemzetek Szervezete Alapokmányának 102. cikkével összhangban. A másik Felet tájékoztatni kell a regisztrációról és az Egyesült Nemzetek Szerződéseinek Tárában szereplő regisztrációs számról, amint azt az Egyesült Nemzetek Szervezetének Titkársága kiadja.

A fentiek hiteléül a Felek megfelelően felhatalmazott képviselői jelen Egyezményt aláírásukkal látták el

2017. október 25. napján Helsinkiben két eredeti példányban, magyar, finn és angol nyelven, mely szövegek mindegyike egyaránt hiteles. Az értelmezés során előforduló bármilyen eltérés esetén az angol nyelvű szöveg az irányadó.

……. ……..
MAGYARORSZÁG **A FINN KÖZTÁRSASÁG**

KORMÁNYA RÉSZÉRŐL

KORMÁNYA RÉSZÉRŐL

1. MELLÉKLET
MINŐSÍTETT SZERZŐDÉSEK

A jelen Egyezmény 6. cikkében említett minősített szerződéseknek tartalmazniuk kell az alábbi információkat:

1. a felhasználót a minősített adat kezelésére feljogosító eljárás;
2. azon jogszabályok és egyéb szabályok, amelyek alapján a minősített adatok felhasználása történik;
3. a szükséges minősítési szint;
4. a minősített adat felhasználásának korlátai;
5. a minősített adat továbbításának módja;
6. a minősített adat kezelésének módja;
7. a minősített adat jelölése és ennek gyakorlati következményei;
8. a minősített adat átvételére feljogosított személyek, beleértve az alvállalkozókat is, valamint a rájuk vonatkozó feltételek;
9. a minősített adat védelmének időtartamára vonatkozó követelmények;
10. a minősített adat megsemmisítésével és visszaküldésével kapcsolatos eljárás.

2. MELLÉKLET
LÁTOGATÁSI KÉRELEM

A jelen Egyezmény 9. cikkében említett látogatási kérelemnek tartalmaznia kell az alábbi információkat:

1. a látogató családi neve, keresztneve, születési helye és ideje, állampolgársága, a látogató beosztása, annak megjelölése, hogy a látogató mely munkáltató képviseletében jár el, azon projekt meghatározása, amelyben a látogató részt vesz, valamint a látogató útlevelének vagy személyazonosító okmányának száma;
2. a látogatás céljának megfelelő, a látogató számára kibocsátott személyi biztonsági tanúsítvány meglétének megerősítése;
3. a látogatás vagy látogatások célja, beleértve a látogatással érintett legmagasabb minősítési szintű minősített adat minősítési szintjét;
4. kérelmezett látogatás vagy látogatások várható időpontja és időtartama, továbbá ismétlődő látogatások esetén a látogatásokkal érintett teljes időszak megjelölése, ha lehetséges;
5. a meglátogatandó létesítmény vagy telephely neve, címe, egyéb elérhetősége és kapcsolattartója, valamint minden olyan információ, amely a látogatás vagy látogatások szükségességének indoklása szempontjából hasznos lehet;
6. dátum, aláírás és a küldő hatáskörrel rendelkező biztonsági hatóság pecsétje.”

„AGREEMENT

BETWEEN

THE GOVERNMENT OF HUNGARY

AND

THE GOVERNMENT OF THE REPUBLIC OF FINLAND

ON MUTUAL PROTECTION OF CLASSIFIED

INFORMATION

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

in order to protect Classified Information related especially to foreign affairs, defence, security, police or scientific, industrial and technological matters and exchanged directly between the Parties, or legal entities or individuals that handle Classified Information under the jurisdiction of the Parties,

have agreed as follows:

ARTICLE 1
PURPOSE AND SCOPE OF APPLICATION

The purpose of this Agreement is to ensure the protection of Classified Information that is exchanged or generated in the process of co-operation between the Parties.

ARTICLE 2
DEFINITIONS

For the purposes of this Agreement:

a) *Classified Information* means any information, document or material of whatever form, nature or method of transmission provided by one Party to the other Party and to which a security classification level has been applied and which has been marked in accordance with the national laws and regulations, as well as any information, document or material that has been generated on the basis of such Classified Information and marked accordingly;

b) *Classified Contract* means any contract or sub-contract, which contains or involves Classified Information;

c) *Contractor* means a legal entity or an individual possessing the legal capacity to conclude classified contracts in accordance with the national laws and regulations;

d) Originating Party means the Party which provides Classified Information or under whose authority Classified Information is generated;

e) *Recipient* means the Party, as well as any legal entity or individual under its jurisdiction, to which the Classified Information is provided by the Originating Party;

f) *Competent Security Authority* means a National Security Authority, a Designated Security Authority or any other competent body authorised in accordance with the national laws and regulations of the Parties which is responsible for the implementation of this Agreement;

g) *Breach of Security* means an act or an omission contrary to national laws and regulations which may lead to the loss or compromise of Classified Information;

h) *Security Clearance* means a positive determination following a vetting procedure to ascertain the eligibility of a legal entity (*Facility Security Clearance*, FSC) or individual (*Personnel Security Clearance*, PSC) to have access to and to handle Classified Information on a certain level in accordance with the national laws and regulations;

i) *Third Party* means any state including the legal entities or individuals under its jurisdiction or international organisation not being a party to this Agreement.

ARTICLE 3
COMPETENT SECURITY AUTHORITIES

1. The National Security Authorities (NSAs) designated by the Parties as responsible for the general implementation of this Agreement are:

In Hungary:	**In the Republic of Finland:**
National Security Authority (NSA) *Nemzeti Biztonsági Felügyelet (NBF)*	*Ministry for Foreign Affairs* *Ulkoasiainministeriö* *National Security Authority (NSA)* *Kansallinen turvallisuusviranomainen*

2. The Parties shall notify each other of any other Competent Security Authorities which shall be responsible for the implementation of aspects of this Agreement.

3. The Parties shall notify each other of any subsequent changes of the Competent Security Authorities.

ARTICLE 4
SECURITY CLASSIFICATIONS

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

2. The classification levels shall correspond to one another as follows:

In Hungary	**In the Republic of Finland**	**English translation**
„Szigorúan titkos!”	ERITTÄIN SALAINEN or YTTERST HEMLIG	TOP SECRET
„Titkos!”	SALAINEN or HEMLIG	SECRET
„Bizalmas!”	LUOTTAMUKSELLINEN or KONFIDENTIELL	CONFIDENTIAL
„Korlátozott terjesztésű!”	KÄYTTÖ RAJOITETTU or BEGRÄNSAD TILLGÅNG	RESTRICTED

3. The Recipient shall ensure that classifications are not altered or revoked, except as authorised in writing by the Originating Party.

ARTICLE 5
PROTECTION OF CLASSIFIED INFORMATION

1. The Parties shall take all appropriate measures in accordance with national laws and regulations so as to protect Classified Information referred to in this Agreement. They shall afford such information the same protection as they afford to their own information at the corresponding classification level.

2. The Parties shall not provide access to Classified Information to Third Parties without the prior written consent of the Originating Party.

3. Access to Classified Information shall be limited to individuals who have a need-to-know and who, in accordance with national laws and regulations, have been security cleared and authorised to have access to such information as well as briefed on their responsibilities for the protection of Classified Information.

4. A Personnel Security Clearance is not required for access to Classified Information at the "Korlátozott terjesztésű!" or KÄYTTÖ RAJOITETTU / BEGRÄNSAD TILLGÅNG level.

5. Classified Information shall be used solely for the purpose for which it has been provided.

ARTICLE 6
CLASSIFIED CONTRACTS

1. Upon request, the Competent Security Authority of the Recipient shall inform the Competent Security Authority of the Originating Party whether a proposed Contractor participating in precontract negotiations or in the implementation of a Classified Contract has been issued an appropriate Security Clearance corresponding to the required security classification level. If the Contractor does not hold such a Security Clearance, the Competent Security Authority of the Originating Party may request that the Contractor be security cleared by the Competent Security Authority of the Recipient.

2. In the case of an open tender the Competent Security Authority of the Recipient may provide the Competent Security Authority of the Originating Party with the relevant Security Clearance certificates without a formal request.

3. A Facility Security Clearance is not required for Classified Contracts at "Korlátozott terjesztésű!" or KÄYTTÖ RAJOITETTU / BEGRÄNSAD TILLGÅNG level.

4. To allow adequate security supervision and control, a Classified Contract shall contain appropriate security provisions as specified in Annex 1, including a security classification guide. A copy of the security provisions shall be forwarded to the Competent Security Authority of the Party under whose jurisdiction the contract is to be performed.

5. Representatives of the Competent Security Authorities of the Parties may visit each other in order to analyse the efficiency of the measures adopted by a Contractor for the protection of Classified Information involved in a Classified Contract.

ARTICLE 7

TRANSMISSION OF CLASSIFIED INFORMATION

1. Classified Information shall be transmitted between the Parties through secured government-to-government channels or as otherwise agreed between their Competent Security Authorities.

2. Classified Information shall be transmitted between the Parties electronically only by secure means agreed between the Competent Security Authorities.

ARTICLE 8
REPRODUCTION, TRANSLATION, AND DESTRUCTION OF CLASSIFIED INFORMATION

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

2. All translations shall contain a suitable annotation, in the language of translation, indicating that they contain Classified Information of the Originating Party.

3. Classified Information marked “Szigorúan titkos!” or ERITTÄIN SALAINEN / YTTERST HEMLIG, or with a corresponding classification level under Article 4, shall be reproduced or translated only upon the written consent of the Originating Party.

4. Classified Information marked “Szigorúan titkos!” or ERITTÄIN SALAINEN / YTTERST HEMLIG, or with a corresponding classification level under Article 4, shall not be destroyed without the prior written consent of the Originating Party. It shall be returned to the Originating Party after it is no longer considered necessary by the Parties.

5. Classified Information marked “Titkos!” or SALAINEN/HEMLIG, or with a corresponding or lower classification level under Article 4, shall be destroyed after it is no longer considered necessary by the Recipient, in accordance with its national laws and regulations.

6. If a crisis situation makes it impossible to protect Classified Information provided under this Agreement, the Classified Information shall be destroyed immediately. The Recipient shall notify the Competent Security Authority of the Originating Party of the destruction of the Classified Information as soon as possible.

ARTICLE 9
VISITS

1. Visits entailing access to Classified Information at “Bizalmas!” or LUOTTAMUKSELLINEN/ KONFIDENTIELL or above require prior written authorisation from the Competent Security Authority of the host Party. Visitors shall only be allowed access where they have been:

a) authorised by the Competent Security Authority of the sending Party to conduct the required visit or visits,

b) granted an appropriate Personnel Security Clearance, and

c) authorised to receive Classified Information in accordance with the national laws and regulations of the host Party.

2. The relevant Competent Security Authority of the requesting Party shall notify the relevant Competent Security Authority of the host Party of the planned visit in accordance with the provisions laid down in this Article, and shall make sure that the latter receives the request for visit at least 14 days before the visit takes place. In urgent cases the Competent Security Authorities may agree on a shorter period. The request for visit shall contain the information specified in Annex 2 to this Agreement.

3. The validity of authorisations for recurring visits shall not exceed 12 months.

ARTICLE 10
SECURITY CO-OPERATION

1. In order to implement this Agreement the National Security Authorities shall notify each other of their relevant national laws and regulations regarding the protection of Classified Information as well as of any subsequent amendments thereto.

2. In order to ensure close co-operation in the implementation of this Agreement the Competent Security Authorities shall consult each other. On request, they shall provide each other with information about their national security standards, procedures and practices for the protection of Classified Information. To this aim the Competent Security Authorities may visit each other.

3. On request, Competent Security Authorities shall, in accordance with national laws and regulations, assist each other in carrying out Security Clearance procedures.

4. The National Security Authorities shall promptly inform each other about changes in relevant Security Clearance certificates.

ARTICLE 11

BREACH OF SECURITY

1. Each Party shall immediately notify the other Party of any suspected or discovered Breach of Security of Classified Information.

2. The Party with jurisdiction shall investigate the incident without delay. The other Party shall, if required, co-operate in the investigation.

3. The Party with jurisdiction shall undertake all possible appropriate measures in accordance with its national laws and regulations so as to limit the consequences of breaches referred to in Paragraph 1 of this Article and to prevent further breaches. The other Party shall be informed of the outcome of the investigation and of the measures undertaken.

ARTICLE 12
COSTS

Each Party shall bear its own costs incurred in the course of implementing its obligations under this Agreement.

ARTICLE 13
RESOLUTION OF DISPUTES

Any dispute between the Parties on the interpretation or application of this Agreement shall be resolved exclusively by means of consultations between the Parties.

ARTICLE 14
RELATIONSHIP WITH OTHER INTERNATIONAL AGREEMENTS

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

ARTICLE 15
FINAL PROVISIONS

1. The Parties shall notify each other of the completion of the national measures necessary for the entry into force of this Agreement. The Agreement shall enter into force on the first day of the second month following the receipt of the later notification.

2. This Agreement shall be in force until further notice. The Agreement may be amended by the mutual, written consent of the Parties. Either Party may propose amendments to this Agreement at any time. If one Party so proposes, the Parties shall begin consultations on amending the Agreement.
3. Either Party may terminate this Agreement by written notification delivered to the other Party through diplomatic channels, observing a period of notice of 6 months. If the Agreement is terminated, any Classified Information already provided and any Classified Information arising under the Agreement shall be handled in accordance with the provisions of the Agreement for as long as necessary for the protection of the Classified Information.

4. After the entry into force of this Agreement, the Party in whose territory the Agreement is concluded shall take immediate measures so as to have the Agreement registered by the Secretariat of the United Nations in accordance with Article 102 of the UN Charter. The other Party shall be notified of the registration and of the registration number in the UN Treaty Series as soon as the UN Secretariat has issued it.

In witness whereof the duly authorised representatives of the Parties have signed this Agreement,

in Helsinki on the 25th of October, 2017

in two original copies, in the Hungarian, Finnish and English languages, each text being equally authentic. In case of any divergence of interpretation, the English text shall prevail.

FOR THE GOVERNMENT OF HUNGARY	**FOR THE GOVERNMENT OF THE REPUBLIC OF FINLAND**

ANNEX 1
CLASSIFIED CONTRACTS

Classified Contracts referred to in Article 6 of this Agreement shall contain the following information:

1. procedure entitling a user to handle Classified Information;

2. laws and regulations forming the base for the use of Classified Information;

3. classification level required;

4. limitations on the use of Classified Information;

5. modalities of transmission of Classified Information;

6. modalities of handling Classified Information;

7. marking of Classified Information and practical consequences thereof;

8. specifications of the persons, including sub-contractors, entitled to receive Classified Information and the conditions therefor;

9. requirements for the period of protecting Classified Information;

10. procedure for destroying or returning Classified Information.

ANNEX 2
REQUEST FOR VISIT

Requests for visit referred to in Article 9 of this Agreement shall contain the following information:

1. the visitor's family name, first name, place and date of birth and nationality, the visitor’s position, with a specification of the employer which the visitor represents, a specification of the project in which the visitor participates, and the visitor's passport number or other identity document number;

2. confirmation of Personnel Security Clearance of the visitor in accordance with the purpose of the visit;

3. the purpose of the visit or visits, including the highest level of Classified Information to be involved;

4. the expected date and duration of the requested visit or visits. In the case of recurring visits the total period covered by the visits shall be stated, when possible;

5. the name, address, other contact information and point of contact of the establishment or facility to be visited, and any other information useful for determining the justification for the visit or visits;

6. the date, signature and stamp/seal of the sending Competent Security Authority.”

4. §

(1) Ez a törvény – a (2) bekezdésben meghatározott kivétellel – a kihirdetését követő napon lép hatályba.
(2) A 2. § és a 3. § az Egyezmény 15. Cikk (1) bekezdésében meghatározott időpontban lép hatályba.
(3) Az Egyezmény, illetve a 2. § és a 3. § 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.

Indokolás a Magyarország Kormánya és a Finn Köztársaság Kormánya között a minősített adatok 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, az Olasz Köztársasággal és a Németországi Szövetségi Köztársasággal kötött általános titokvédelmi egyezményt[1] amelyek alkalmazását a 2010. március 31-ig hatályos, az államtitokról és szolgálati titokról szóló 1995. évi LXV. törvény nem tette lehetővé.
A Mavtv. 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[2]. Ennek megfelelően hazánk a 46/2011. (VI. 21.) ME határozat értelmében először a Szlovák Köztársasággal, a Lengyel Köztársasággal és a Cseh Köztársasággal kezdte meg a tárgyalásokat, amelyek eredményeképpen 2012. május 3-án aláírásra került Budapesten a Szlovák Köztársaság és Magyarország, 2012. június 13-án a Cseh Köztársaság és Magyarország, 2014. január 29-én a Lengyel Köztársaság és Magyarország közötti megállapodás. Továbbá az 58/2012. (V. 16.) ME határozat alapján 2012. augusztus 29-én a Lett Köztársaság és Magyarország, 2012. december 11-én a Francia Köztársaság és Magyarország, 2013. március 22-én az Osztrák Köztársaság és Magyarország között hasonló megállapodást, valamint az 54/2013. ME határozat alapján

1 Ld. 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. törvényt, valamint a Magyar Köztársaság Kormánya és 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. törvényt.

2 Egy NATO, EU tagállam a NATO, EU tagállami kört lefedő, és az adott ország külpolitikai és gazdasági orientációjához igazodó kétoldalú titokvédelmi megállapodások széles körével rendelkezik.

2014. július 3-án a Macedón Köztársaság és Magyarország, 2014. szeptember 8-án az Albán Köztársaság és Magyarország között jött létre a minősített adatok cseréjéről és kölcsönös védelméről szóló egyezmény. Az 58/2012. (V. 16.) ME határozat alapján létrehozásra került a Belga Királyság és Magyarország közötti megállapodás, amelynek aláírására 2015. szeptember 21-én került sor, az 54/2013. (IV. 16.) ME határozat alapján pedig a Ciprusi Köztársaság és Magyarország közötti megállapodás jött létre, amelynek aláírására 2015. október 29-én került sor. 2015. november 25-én aláírásra került az 58/2012. (V. 16.) ME határozat alapján létrehozott megállapodás Magyarország és az Olasz Köztársaság között. Az 54/2013. (IV. 10.) ME határozat alapján 2016-ban hat megállapodás aláírására került sor; 2016. január 22-én a Szlovén Köztársasággal, 2016. június 10-én a Horvát Köztársasággal, 2016. június 15-én Spanyolországgal, 2016. szeptember 7-én az Orosz Föderációval, 2016. október 6-án Montenegróval, valamint 2016. december 8-án Észtországgal. 2017. július 5-én került aláírásra a minősített adatvédelmi megállapodás a Bolgár Köztársasággal, 2017. október 25-én pedig a Svéd Királysággal.

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

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 magyar és angol nyelvű hiteles szövegét.

Az Egyezmény célja, hogy védelmet biztosítson a Felek, valamint a joghatóságuk alá tartozó állami szervek, illetve egyéb, például gazdasági szervezetek 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 4-5. §-hoz

A Javaslat – a 2. és 3. § kivételével – a kihirdetését követő napon lép hatályba. A 2. § és a 3. § hatálybalépése az Egyezmény hatálybalépéséhez igazodik. Az Egyezmény szerint „a Felek tájékoztatják egymást a jelen Egyezmény hatálybalépéséhez szükséges nemzeti intézkedéseik teljesítéséről. Jelen Egyezmény az erről szóló későbbi értesítés kézhezvételét 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 kerül sor. Az Egyezmény hatálybalépésének naptári napját a külpolitikáért felelős miniszter annak ismertté válását követően a Magyar Közlönyben közzétett egyedi közleményével állapítja meg.