MAGYARORSZÁG KORMÁNYA

Átiktatva: T/408.

~~**T/20374. számú**~~

törvényjavaslat

a Magyarország Kormánya és a Svéd Királyság Kormánya között a minősített adatok cseréjéről és kölcsönös védelméről szóló egyezmény kihirdetéséről

Előadó: Dr. Pintér Sándor
belügyminiszter

Budapest, 2018. március

2018. évi … törvény

a Magyarország Kormánya és a Svéd Királyság Kormánya között a minősített adatok cseréjéről és kölcsönös védelméről szóló egyezmény kihirdetéséről

1. §

Az Országgyűlés e törvénnyel felhatalmazást ad a Magyarország Kormánya és a Svéd Királyság 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 angol nyelvű szövege a következő:

„EGYEZMÉNY
MAGYARORSZÁG KORMÁNYA
ÉS
A SVÉD KIRÁLYSÁG KORMÁNYA
KÖZÖTT

A MINŐSÍTETT ADATOK CSERÉJÉRŐL ÉS KÖLCSÖNÖS VÉDELMÉRŐL

Magyarország Kormánya és a Svéd Királyság Kormánya (a továbbiakban együtt: „a Felek”),

Elismerve a kölcsönös együttműködés fontos szerepét,

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

Elismerve, hogy azonos szintű védelmet biztosítanak a minősített adatok számára,

Új változattal kívánva kicserélni a Magyar Köztársaság Kormánya és a Svéd Királyság Kormánya között a katonai minősített adatok védelme tárgyában Budapesten, 1995. október 13-án aláírt Egyezményt,

Kívánatosnak tartva a közöttük, valamint a joghatóságuk alá tartozó jogi személyek között kicserélt minősített adatok védelmének biztosítását,

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

1. Cikk
Az Egyezmény tárgya

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

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

2. Cikk
Fogalommeghatározások

Jelen Egyezmény alkalmazásában:

a) A minősített adat: megjelenési formájától vagy természetétől függetlenül, minden olyan adat, amelyet bármelyik Fél nemzeti jogszabályai szerint védelemben kell részesíteni az illetéktelen tudomásra jutástól.

b) A minősített szerződés: olyan szerződés, amely minősített adatot tartalmaz, vagy amely alapján minősített adathoz való hozzáférés szükséges.

c) Az átadó fél: az a Fél, valamint a joghatósága alá tartozó jogi személy vagy természetes személy, amelyik a minősített adatot átadja.

d) Az átvevő fél: az a Fél, valamint a joghatósága alá tartozó jogi személy vagy természetes személy, amelyik a minősített adatot átveszi.

e) A harmadik fél: bármely olyan állam, valamint a joghatósága alá tartozó jogi személy vagy természetes személy, továbbá nemzetközi szervezet, amely nem részese jelen Egyezménynek.

f) A szükséges ismeret elve: az a követelmény, amely alapján a minősített adathoz való hozzáférés csak annak a személynek biztosítható, akinek a hozzáférés hivatali feladata ellátásához szükséges.

g) Illetéktelen tudomásra jutás: a minősített adat bármilyen formájú jogosulatlan felhasználása, megsértése vagy jogosulatlan hozzáférése, megváltoztatása, nyilvánosságra hozatala, megsemmisítése, valamint minden egyéb intézkedés vagy intézkedés elmulasztása, melynek eredményeként sérül a minősített adat bizalmassága, sérthetetlensége vagy hozzáférhetősége.

h) Védelmi hatóságok: a Svéd Királyság azon hatóságai, amelyekre a Svéd Fegyveres Erők védelmi biztonsági szabályait kell alkalmazni.

i) Egyéb hatóságok: a Svéd Királyság azon hatóságai, amelyekre a Svéd Biztonsági Szolgálat védelmi biztonsági szabályait kell alkalmazni.

3. Cikk
Minősítési szintek megfeleltetése

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

Magyarországon	A Svéd Királyságban	
	Védelmi Hatóságok	Egyéb Hatóságok
„Szigorúan titkos!”	HEMLIG/ TOP SECRET	HEMLIG AV SYNNERLIG BETYDELSE FÖR RIKETS SÄKERHET
„Titkos!”	HEMLIG/ SECRET	HEMLIG
„Bizalmas!”	HEMLIG/ CONFIDENTIAL	-
„Korlátozott terjesztésű!”	HEMLIG/ RESTRICTED	-

(2) A Magyarország által átadott „Bizalmas!” vagy „Korlátozott terjesztésű!” minősítéssel ellátott adatot úgy kell kezelni, mint a Svéd Királyság egyéb hatóságai által HEMLIG minősítéssel ellátott adatot.

(3) Az átadó fél haladéktalanul tájékoztatja az átvevő felet az átadott minősített adat minősítésében bekövetkezett valamennyi változásról.

(4) Az átadó fél:

a) biztosítja, hogy a minősített adat a nemzeti jogszabályok és egyéb szabályok rendelkezéseinek megfelelő minősítéssel legyen ellátva;

b) értesíti az átvevő felet a minősített adat nyilvánosságra hozatalának, hozzáférésének vagy felhasználásának feltételeiről.

(5) Az átvevő fél biztosítja, hogy a minősített adat jelen Cikk 1. bekezdése szerint, a megfelelő nemzeti minősítéssel legyen ellátva.

(6) A Felek értesítik egymást a nemzeti minősítésekben bekövetkezett valamennyi változásról.

4. Cikk
A minősített adat védelme

(1) A Felek megteszik a vonatkozó nemzeti jogszabályai és egyéb szabályai rendelkezéseinek megfelelő intézkedéseket annak érdekében, hogy az átvett minősített adat jelen Egyezmény 3. Cikkében meghatározott minősítési szintek szerint a megfelelő szintű védelemben részesüljön.

(2) Jelen Egyezmény nem sértheti a Felek azon nemzeti jogszabályainak és egyéb szabályainak rendelkezéseit, amelyek a közérdekű adatokhoz vagy közérdekből nyilvános adatokhoz való hozzáférésről, a személyes adatok védelméről és a minősített adatok védelméről szólnak.

(3) Mindkét Fél köteles nemzeti jogszabályai rendelkezéseivel összhangban biztosítani a megfelelő intézkedések foganatosítását a minősített adatok védelme érdekében azok, kommunikációs vagy információs rendszerekben való felhasználása, tárolása vagy továbbítása során. Ezen intézkedéseknek biztosítaniuk kell a minősített adat bizalmasságát, sértetlenségét, rendelkezésre állását és amennyiben szükséges a minősített adat letagadhatatlanságát, és hitelességét, valamint az adattal kapcsolatos intézkedések elszámoltathatóságának és nyomon követhetőségének megfelelő szintjét.

(4) A hatáskörrel rendelkező biztonsági hatóságok szükség esetén tájékoztatják egymást azon speciális biztonsági kockázatokról, amelyek az átvett minősített adat biztonságát veszélyeztethetik.

5. Cikk
Minősített adat közlése és felhasználása

(1) Mindkét Fél köteles biztosítani, hogy a jelen Egyezmény alapján átadott vagy továbbított minősített adat:

a) csak az átadó fél által meghatározott célra legyen felhasználva;

b) harmadik országnak vagy nemzetközi szervezettel való közlése csak az átadó fél előzetes, írásbeli engedélyével, és az átvevő fél valamint az érintett harmadik ország vagy nemzetközi szervezet között, a minősített adatok védelmére vonatkozó egyezmény vagy intézkedés szerint történhessen meg.

(2) Az átvevő fél csak az átadó fél előzetes, írásbeli engedélyével és az általa előzetesen végrehajtott visszaminősítéssel vagy a minősítés előzetes megszüntetésével kezdeményezheti jelen Egyezmény alapján létrejött vagy továbbított minősített adat visszaminősítését, vagy a minősítés megszüntetését.

(3) A minősítő hozzájárulásának alapelvét valamennyi Fél köteles betartani az alkotmányos követelményeivel, valamint a nemzeti jogszabályok és egyéb szabályok rendelkezéseivel összhangban.

6. Cikk
Minősített adathoz való hozzáférés

(1) A Felek biztosítják, hogy jelen Egyezmény alapján létrejött vagy továbbított minősített adathoz való hozzáférés csak a szükséges ismeret elve alapján, és a nemzeti jogszabályok és egyéb szabályok rendelkezéseivel összhangban történjen.

(2) A Felek biztosítják, hogy minden személy, aki jelen Egyezmény alapján létrehozott vagy továbbított minősített adathoz hozzáfér, a nemzeti jogszabályok és egyéb szabályok rendelkezései alapján tájékoztatva legyen az adatok védelmével kapcsolatos kötelezettségeiről.

(3) A Felek biztosítják, hogy a „Bizalmas!”/ HEMLIG/ CONFIDENTIAL vagy annál magasabb minősítéssel ellátott minősített adathoz való hozzáférésre csak az a személy kapjon jogosultságot, aki a megfelelő szintű személyi biztonsági tanúsítvánnyal vagy feladatai alapján más, a nemzeti jogszabályok és egyéb szabályok rendelkezéseinek megfelelő felhatalmazással rendelkezik.

(4) A Felek nemzeti jogszabályainak és egyéb szabályainak rendelkezéseivel összhangban biztosítják, hogy a joghatóságuk alá tartozó jogi személyek megfeleljenek a biztonsági előírásoknak és képesek legyenek jelen Egyezmény 4. cikk 1. bekezdésében előírtaknak megfelelő védelmet biztosítani, a megfelelő minősítési szinten, ha minősített adatot vesznek át vagy hoznak létre.

7. Cikk
A hatáskörrel rendelkező biztonsági hatóságok és biztonsági együttműködések

(1) Jelen Egyezmény vonatkozásában, a hatáskörrel rendelkező biztonsági hatóságok a következők:

Magyarországon:

Nemzeti Biztonsági Felügyelet
(National Security Authority)

A Svéd Királyságban:

Försvarsmakten, Militära säkerhetstjänsten
(National Security Authority)

Försvarets materielverk
(Designated Security Authority)

(2) A Felek írásban tájékoztatják egymást hatáskörrel rendelkező biztonsági hatóságaik hivatalos elérhetőségi adatairól.

(3) A Felek írásban tájékoztatják egymást a hatáskörrel rendelkező biztonsági hatóságokat érintő valamennyi változásról.

(4) Összeegyeztethető szintű biztonsági követelmények fenntartása érdekében a hatáskörrel rendelkező biztonsági hatóságok a másik Fél megkeresésére tájékoztatják egymást a minősített adat védelmével kapcsolatos nemzeti jogszabályokról, valamint mindezek gyakorlati alkalmazásáról. A hatáskörrel rendelkező hatóságok tájékoztatják egymást az Egyezménnyel kapcsolatban felmerülő valamennyi, lényeges változásról. A fentiek érdekében, az Egyezmény időtartama alatt a hatáskörrel rendelkező hatóságok látogatást folytathatnak le a másik Fél hatáskörrel rendelkező biztonsági hatóságainál.

(5) A Felek kölcsönösen elismerik a másik Fél által kibocsátott személyi biztonsági tanúsítványokat és telephely biztonsági tanúsítványokat, és haladéktalanul tájékoztatják egymást a kölcsönösen elismert biztonsági tanúsítványokat érintő valamennyi változásról.

(6) Megkeresés esetén a Felek kölcsönösen segítséget nyújtanak egymásnak a személyi biztonsági tanúsítványokkal és a telephely biztonsági tanúsítványokkal kapcsolatos eljárások során.

(7) Felek értesítik egymást az intézkedés okainak megjelölésével, ha valamelyik hatáskörrel rendelkező biztonsági hatóság felfüggeszti a minősített adatokhoz való hozzáférést, vagy ilyen célból intézkedést foganatosít olyan minősített adatra vonatkozóan, amelyhez a másik Fél országának állampolgára egyébként személyi biztonsági tanúsítványa alapján jogosult lenne hozzáférni.

(8) Jelen Egyezmény alapján megvalósuló együttműködés angol nyelven történik.

8.Cikk
Minősített Szerződések

(1) A minősített szerződéseket a Felek saját nemzeti jogszabályainak és egyéb szabályainak rendelkezései alapján kell megkötni és teljesíteni. A hatáskörrel rendelkező biztonsági hatóságok megkeresésre megerősítik, 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 biztonsági hatóságok kérelmezhetik, hogy a másik Fél biztonsági ellenőrzést folytasson le a területén működő létesítményben a minősített adat folyamatos védelmének biztosítása céljából.

(3) A minősített szerződéseknek tartalmazniuk kell a biztonsági követelményekre és a minősített szerződés elemeinek minősítési szintjére vonatkozó intézkedéseket is. Ezen intézkedések másolatát azon Fél hatáskörrel rendelkező biztonsági hatósága részére kell továbbítani, amelynek joghatósága alatt a minősített szerződés végrehajtása történik.

9. Cikk
A minősített adat továbbítása

(1) A minősített adat továbbítása az átadó fél nemzeti jogszabályai szerint, diplomáciai úton, vagy a hatáskörrel rendelkező biztonsági hatóságok által kölcsönösen elfogadott egyéb módon történik, a „Korlátozott terjesztésű!”/ HEMLIG/ RESTRICTED minősítéssel ellátott minősített adat kivételével, amely az átadó fél nemzeti jogszabályainak és egyéb szabályainak rendelkezéseivel összhangban más módon is továbbítható.

(2) A Felek a hatáskörrel rendelkező biztonsági hatóságok által jóváhagyott eljárási rend szerint, elektronikus úton is továbbíthatnak minősített adatot.

(3) Jelen Egyezmény végrehajtása érdekében a Felek külön megállapodhatnak biztonságos kommunikációt eredményező intézkedések bevezetéséről a minősített adatok elektronikus úton történő biztonságos továbbításának és a Felek közötti biztonságos kommunikáció szabályozásának céljából.

10. Cikk
A minősített adat sokszorosítása, fordítása és megsemmisítése

(1) Jelen Egyezmény alapján átadott vagy kicserélt minősített adatról készült másolatokon és fordításokon fel kell tüntetni a megfelelő minősítést 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 vagy kicserélt minősített adat fordítása során keletkező példányokon a fordítás nyelvén fel kell tüntetni, hogy az átadó fél minősített adatát tartalmazza.

(3) A Jelen Egyezmény alapján átadott vagy kicserélt „Szigorúan titkos!”/ HEMLIG/ TOP SECRET minősítési szintű adat fordítása vagy sokszorosítása kizárólag az átadó fél előzetes írásbeli engedélyével lehetséges.

(4) Jelen Egyezmény alapján átadott vagy kicserélt „Szigorúan titkos!”/ HEMLIG/ TOP SECRET minősítési szintű adat nem semmisíthető meg, az ezen minősítési szintű adatokat az átadó félnek kell visszaszolgáltatni azt követően, hogy azokat az átvevő fél már nem tekinti szükségesnek.

(5) A „Titkos!”/ HEMLIG/ SECRET minősítési szintű minősített adatot a nemzeti jogszabályok és egyéb szabályok rendelkezései szerint kell megsemmisíteni azt követően, hogy az átvevő fél már nem tekinti azt szükségesnek.

(6) Olyan veszélyhelyzet esetén, amikor jelen Egyezmény alapján átadott vagy kicserélt minősített adat minősítésének megfelelő védelme lehetetlenné válik, vagy lehetetlen az átadó félhez való visszajuttatása, a minősített adatot azonnal meg kell semmisíteni. Ebben az esetben az átvevő fél hatáskörrel rendelkező biztonsági hatósága, amint lehetséges értesíti az átadó fél hatáskörrel rendelkező biztonsági hatóságát a minősített adat megsemmisítéséről.

11. Cikk
Látogatások

(1) Minősített adathoz való hozzáférést igénylő látogatásra az érintett hatáskörrel rendelkező biztonsági hatóság előzetes írásbeli jóváhagyása alapján kerülhet sor kivéve, ha a hatáskörrel rendelkező biztonsági hatóságok másként állapodtak meg.

(2) A látogatásra vonatkozó megkeresést legalább húsz (20) nappal a látogatás időpontja előtt kell benyújtani. Sürgős esetben, a hatáskörrel rendelkező biztonsági 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 intézmény 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) ha szükséges, annak a projektnek leírása, amelyben a látogató részt vesz;

g) meglátogatandó létesítmény neve és címe, valamint a kapcsolattartójának neve, telefonszáma, fax száma, e-mail címe;

h) a hatáskörrel rendelkező hatóságok megegyezése eredményeként szükségessé vált egyéb adat;

i) dátum, és a hatáskörrel rendelkező hatóság aláírása.

(4) A hatáskörrel rendelkező biztonsági hatóságok közösen meghatározhatják a visszatérő látogatásra jogosult személyek listáját. A visszatérő látogatások további részleteit a hatáskörrel rendelkező biztonsági hatóságok közösen állapítják meg.

(5) A látogatónak átadott minősített adatot úgy kell tekinteni, mint a jelen Egyezmény alapján átvett minősített adatot.

(6) A látogató köteles betartani a fogadó fél biztonsági előírásait.

12. Cikk
Eljárás a minősített adat biztonságának megsértése esetén

(1) A hatáskörrel rendelkező biztonsági hatóságok késedelem nélkül írásban tájékoztatják egymást a minősített adat biztonságának megsértéséről, ha a jelen Egyezmény hatálya alá tartozó minősített adat jogosulatlan nyilvánosságra hozatalára, jogosulatlan megváltoztatására kerül sor, vagy mindezek alapos gyanúja merül fel.

(2) Azon Fél hatáskörrel rendelkező biztonsági hatósága, amelynek területén a minősített adat biztonságának megsértésére sor került, késedelem nélkül intézkedik a minősített adat megsértésének kivizsgálása érdekében. A másik Fél hatáskörrel rendelkező biztonsági hatósága felkérés esetén részt vesz a vizsgálatban.

(3) Az átvevő fél hatáskörrel rendelkező biztonsági hatósága 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.

13. Cikk
Költségek viselése

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 által az Egyezmény hatálybalépéshez szükséges nemzeti jogi feltételek teljesítésére vonatkozó, diplomáciai úton küldött utolsó értesítés kézhezvételének napját követő második hónap első napján lép hatályba.

(2) Jelen Egyezmény hatályba lépésével a Magyar Köztársaság Kormánya és a Svéd Királyság Kormánya között a katonai minősített adatok védelme tárgyában Budapesten, 1995. október 13-án aláírt Egyezmény hatályát veszti.

(3) Jelen Egyezmény a Felek kölcsönös egyetértésével írásban módosítható. A módosítások hatálybalépésével kapcsolatban a jelen Cikk 1. pontjában foglaltak az irányadók.

(4) Bármelyik Fél jogosult jelen Egyezményt bármikor írásban felmondani. Felmondás esetén a felmondásról szóló írásbeli értesítés másik Fél általi kézhezvételétől számított hat (6) hónap elteltével hatályát veszti.

(5) Az Egyezmény megszűnésétől függetlenül az annak alapján kicserélt vagy keletkezett 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.

(6) Felek a jelen Egyezmény értelmezéséből vagy végrehajtásából fakadó vitákat egyeztetés és tárgyalás útján, harmadik fél vagy nemzetközi bíróság igénybevétele nélkül rendezik.

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

Készült Budapesten, 2017. október 25-én, két eredeti példányban, magyar, svéd és angol nyelven, valamennyi szöveg egyaránt hiteles. Eltérő értelmezés esetén az angol nyelvű szöveg az irányadó.

Magyarország Kormánya részéről

a Svéd Királyság Kormánya részéről

„AGREEMENT
BETWEEN
THE GOVERNMENT OF HUNGARY
AND
THE GOVERNMENT OF THE KINGDOM OF SWEDEN
ON EXCHANGE AND MUTUAL PROTECTION
OF CLASSIFIED INFORMATION

The Government of Hungary and the Government of the Kingdom of Sweden (hereinafter referred to as the "Parties"),

Recognising the important role of mutual cooperation,

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 replace the Agreement between the Government of the Republic of Hungary and the Government of the Kingdom of Sweden concerning security measures for the protection of classified military data, done in Budapest on 13 October 1995,

Wishing to ensure the protection of Classified Information exchanged between them or between legal entities under their jurisdiction,

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

ARTICLE 1
SCOPE OF THE AGREEMENT

1. The objective of this Agreement is to ensure the protection of Classified Information exchanged or generated in the course of co-operation between the Parties or between legal entities under their jurisdiction.

2. 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 2
DEFINITIONS

For the purpose of this Agreement:

a) **"Classified Information"** means any information that, regardless of its form or nature, under the national legislation of either Party, requires protection against compromise.

b) **"Classified Contract"** means a contract that involves or requires access to Classified Information.

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

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

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

f) "**Need-to-know principle**" means a principle by which access to Classified Information may be granted to an individual in order to be able to perform official duties and tasks.

g) **"Compromise**" means any form of misuse, damage or unauthorized access, alteration, disclosure or destruction of Classified Information, as well as any other action or inaction, resulting in loss of its confidentiality, integrity or availability.

h) **"Defence Authorities**" means authorities in the Kingdom of Sweden for which the Swedish Armed Forces' Protective security regulations apply.

i) **"Other Authorities**" means authorities in the Kingdom of Sweden for which the Swedish Security Service Protective security regulations apply.

ARTICLE 3
SECURITY CLASSIFICATION LEVELS AND MARKINGS

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

In Hungary	In the Kingdom of Sweden	
	Defence Authorities	Other Authorities
„Szigorúan titkos!"	HEMLIG/TOP SECRET	HEMLIG AV SYNNERLIG BETYDELSE FÖR RIKETS SÄKERHET
„Titkos!"	HEMLIG/SECRET	HEMLIG
„Bizalmas!"	HEMLIG/CONFIDENTIAL	—
„Korlátozott terjesztésű!"	HEMLIG/RESTRICTED	—

2. Information from Hungary bearing the marking „Bizalmas!" or „Korlátozott terjesztésű!" shall be treated as HEMLIG by Other Authorities in the Kingdom of Sweden.

3. The Originating Party shall without delay notify the Recipient Party of any changes to the security classification of released Classified Information.

4. The Originating Party shall:

   a) ensure that Classified Information is marked with an appropriate security classification marking in accordance with its national laws and regulations,

   b) inform the Recipient Party of any conditions of release or limitations on the use of Classified Information.

5. The Recipient Party shall ensure that Classified Information is marked with an equivalent national classification marking in accordance with Paragraph 1 of this Article.

6. The Parties shall notify each other of any changes to national security classification markings.

ARTICLE 4

PROTECTION OF CLASSIFIED INFORMATION

1. The Parties shall take all appropriate measures in accordance with their respective national laws and regulations to ensure that the level of protection afforded to Classified Information received shall be in accordance with their equivalent security classification level as stated in Article 3 of this Agreement.

2. Nothing in this Agreement shall cause prejudice to the national laws and regulations of the Parties regarding public access to documents or access to information of public character, the protection of personal data or the protection of Classified Information.

3. Each Party shall, in accordance with national laws and regulations, ensure that appropriate measures are implemented for the protection of Classified Information processed, stored or transmitted in communication and information systems. Such measures shall ensure the confidentiality, integrity, availability and, where applicable, non-repudiation and authenticity of Classified Information, as well as an appropriate level of accountability and traceability of actions in relation to that information.

4. The competent security authorities shall inform each other of specific security risks that may endanger released Classified Information, as applicable.

ARTICLE 5

DISCLOSURE AND USE OF CLASSIFIED INFORMATION

1. Each Party shall ensure that Classified Information provided or exchanged under this Agreement is:

a) used only for purposes established by the Originating Party,

b) not disclosed to any third state or international organisation without the prior written consent of the Originating Party, and an appropriate agreement or arrangement for the protection of Classified Information between the Recipient Party and the third state or international organisation concerned.

2. The Recipient Party shall only execute a downgrading or declassification of Classified Information provided or exchanged under this Agreement after the prior written consent of, and prior downgrading or prior declassification by, the Originating Party.

3. The principle of originator consent shall be respected by each Party in accordance with its constitutional requirements, national laws and regulations.

ARTICLE 6
ACCESS TO CLASSIFIED INFORMATION

1. Each Party shall ensure that access to Classified Information provided or exchanged under this Agreement is granted on the basis of the Need-to-know principle in accordance with national laws and regulations.

2. Each Party shall ensure that all individuals granted access to Classified Information provided or exchanged under this Agreement are informed of their responsibilities to protect such information in accordance with national laws and regulations.

3. The Parties shall guarantee that access to Classified Information bearing the classification marking „Bizalmas!”/HEMLIG/CONFIDENTIAL or above is granted only to individuals who hold an appropriate security clearance or who are otherwise duly authorised by virtue of their functions in accordance with national laws and regulations.

4. In accordance with its national laws and regulations, each Party shall ensure that any entity under its jurisdiction that may receive or generate Classified Information is appropriately security cleared and is capable of providing suitable protection, as provided for in Paragraph 1 of Article 4 of this Agreement, at the appropriate security level.

ARTICLE 7
COMPETENT SECURITY AUTHORITIES AND SECURITY CO-OPERATION

1. For the purpose of this Agreement, the competent security authorities are:

In Hungary:

Nemzeti Biztonsági Felügyelet
(National Security Authority)

In the Kingdom of Sweden:

Försvarsmakten, Militära säkerhetstjänsten
(National Security Authority)

Försvarets materielverk
(Designated Security Authority)

2. Each Party shall provide the other with the necessary contact data of their respective competent security authorities in writing.

3. The Parties shall inform each other, in writing, of any subsequent changes of their respective competent security authorities.

4. In order to maintain comparable standards of security, the competent security authorities shall, on request, inform each other of their national legislation concerning the protection of Classified Information and the practices stemming from their implementation. The competent security authorities shall inform each other of any substantive changes concerning the Agreement. To this end, the competent security authorities may conduct mutual visits.

5. The Parties shall mutually recognise each other's respective personnel and facility security clearances, and promptly inform each other about any changes in the mutually recognised security clearances.

6. Upon request, the Parties shall provide mutual assistance in carrying out security clearance procedures.

7. If either competent security authority suspends or takes action to revoke access to Classified Information that has been granted to a citizen of the other Party based upon a security clearance, the other Party will be notified and given the reasons for such an action.

8. The co-operation under this Agreement shall be effected in the English language.

ARTICLE 8
CLASSIFIED CONTRACTS

1. Classified Contracts shall be concluded and implemented in accordance with the national laws and regulations of each Party. On request, the competent security authorities shall confirm that

proposed contractors as well as individuals participating in pre-contractual negotiations or in the implementation of Classified Contracts have appropriate personnel security clearance or facility security clearance.

2. The competent security authority may request its counterpart that a security inspection is carried out at a facility located in the territory of the other Party to ensure continuing protection of Classified Information.

3. Classified Contracts shall contain provisions on the security requirements and on the security classification level of each element of the Classified Contract. A copy of these provisions shall be forwarded to the competent security authority of the Party under whose jurisdiction the Classified Contract is to be implemented.

ARTICLE 9
TRANSFER OF CLASSIFIED INFORMATION

1. Classified Information shall be transferred in accordance with the national legislation of the Originating Party through diplomatic channels or as otherwise mutually approved between the competent security authorities, except Classified Information marked as „Korlátozott terjesztésű!"/HEMLIG/RESTRICTED, which may be transferred or transmitted also by other means in accordance with national laws and regulations of the Originating Party.

2. The Parties may transmit Classified Information by electronic means in accordance with the security procedures approved by the competent security authorities.

3. The Parties may, for implementation of this Agreement, mutually agree on a separate communication security arrangement for the purpose of regulating secure electronic transmission of Classified Information and secure communication between them.

ARTICLE 10
REPRODUCTION, TRANSLATION AND DESTRUCTION OF CLASSIFIED INFORMATION

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

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

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

4. Classified Information provided or exchanged under this Agreement marked „Szigorúan titkos!"/HEMLIG/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.

5. Information classified „Titkos!”/HEMLIG/SECRET or below shall be destroyed after it is no longer considered necessary by the Recipient Party, in accordance with national laws and regulations.

6. In case of any crisis situation which makes it impossible to protect Classified Information provided or exchanged under this Agreement according to its marking, or if it is impossible to return, the Classified Information shall be destroyed immediately. In such a case the competent security authorithy of the Recipient Party shall notify the competent security authority of the Originating Party about the destruction as soon as possible.

ARTICLE 11
VISITS

1. Visits requiring access to Classified Information shall be subject to the prior written approval of the respective competent security authority unless otherwise mutually approved by the competent security authorities.

2. Requests for visit shall be submitted at least twenty (20) 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 competent security authorities.

3. Requests for visit shall contain:

a) visitor’s name, date and place of birth, citizenship and passport/ID card number,

b) position of the visitor and specification of the legal entity represented,

c) visitor’s personnel security clearance status and its validity,

d) date and duration of the visit, in case of recurring visits the total period of time covered by the visits,

e) purpose of the visit including the highest security classification level of Classified Information involved,

f) specification of the project in which the visitor is participating, if applicable,

g) 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,

h) other data, if agreed upon by the competent security authorities,

i) date and signature of the competent security authority.

4. The competent security authorities may agree on a list of visitors entitled to recurring visits. The competent security authorities shall agree on the further details of the recurring visits.

5. Classified Information provided to a visitor shall be considered as Classified Information received under this Agreement.

6. A visitor shall comply with the security regulations of the host Party.

ARTICLE 12
BREACH OF SECURITY

1. The competent security authorities shall without undue delay inform each other in writing of a breach of security resulting in unauthorised disclosure or any other unauthorised manipulation of Classified Information under this Agreement or suspicion thereof.

2. The competent security authority of the Party where the breach of security occurred, shall investigate the incident without delay. The other competent security authority shall, if required, co-operate in the investigation.

3. In any case, the competent security authority of Recipient Party shall inform 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

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 notification between the Parties, through diplomatic channels, stating that the national legal requirements for this Agreement to enter into force have been fulfilled.

2. As of the date of entry into force of this Agreement, the Agreement between the Government of the Republic of Hungary and the Government of the Kingdom of Sweden concerning security measures for the protection of classified military data, done in Budapest on 13 October 1995, shall terminate as between the Parties.

3. 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.

4. Each Party is entitled to terminate this Agreement in writing at any time. In such a case, the validity of this Agreement shall expire after six (6) months following the day on which the other Party receives the written notice of the termination.

5. Regardless of the termination of this Agreement, all Classified Information exchanged or generated under this Agreement shall be protected in accordance with the provisions set forth herein until the Originating Party dispenses the Recipient Party from this obligation in writing.

6. Any dispute regarding the interpretation or implementation of this Agreement shall be resolved by consultations and negotiations between the Parties, without recourse to a third party or an international tribunal for settlement.

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

Done in Budapest on **25th of October 2017** in two originals, each in the Hungarian, Swedish and English languages, all texts being equally authentic. In case of different interpretation the English text shall prevail.

On behalf of the Government of Hungary	**On behalf of the Government of the Kingdom of Sweden**

4. §

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

(2) A 2. § és a 3. § az Egyezmény 14. 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 Svéd Királyság 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, 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 alá-

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.

írásra 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 kötött hasonló megállapodást, valamint az 54/2013. ME határozat alapján 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 három megállapodás aláírására került sor; 2016. január 22-én a Szlovén Köztársasággal, 2016. június 10-én a Horvát Köztársasággal és 2016. június 15-én Spanyolországgal.
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 Szerződő 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. §-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 „a Felek által az Egyezmény hatálybalépéshez szükséges belső eljárások lefolytatásáról szóló, diplomáciai úton küldött utolsó írásbeli értesítés 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 kerül sor. Az Egyezmény hatálybalépésének naptári napját a külpolitikáért felelős miniszter annak ismertté válását követően a Magyar Közlönyben közzétett egyedi közleményével állapítja meg.

az 5. §-hoz

Figyelemmel az Egyezmény tartalmára a minősített adatok védelmének szakmai felügyeletéért felelős miniszter kijelölése indokolt a végrehajtáshoz szükséges intézkedések megtétele érdekében.