MAGYARORSZÁG KORMÁNYA

T/1654. számú

törvényjavaslat

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

Előadó: **Dr. Pintér Sándor**
belügyminiszter

Budapest, 2018. szeptember

2018. évi … törvény

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

1. §

Az Országgyűlés e törvénnyel felhatalmazást ad a Magyarország Kormánya és a Németországi Szövetségi Köztársaság Kormánya között létrejött, 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 NÉMETORSZÁGI SZÖVETSÉGI KÖZTÁRSASÁG KORMÁNYA

KÖZÖTT

A MINŐSÍTETT ADATOK KÖLCSÖNÖS VÉDELMÉRŐL

Magyarország Kormánya

és

a Németországi Szövetségi Köztársaság Kormánya

(a továbbiakban együtt: „Szerződő Felek”),

biztosítani kívánva Magyarország és a Németországi Szövetségi Köztársaság hatáskörrel rendelkező hatóságai, valamint az egyik Szerződő Fél hatósága és a másik Szerződő Fél területén lévő szerződő, továbbá a Szerződő Felek szerződői között kicserélt minősített adatok védelmét,

a minősített adatok kölcsönös védelméről szóló megegyezés létrehozását kívánva, amely egyaránt alkalmazandó a Szerződő Felek között kötendő valamennyi együttműködési megállapodásra és a minősített adatok cseréjét érintő szerződésekre,

új egyezménnyel kívánva kiváltani a Magyar Köztársaság Kormánya és a Németországi Szövetségi Köztársaság Kormánya között a minősített információk kölcsönös védelme tárgyában 1995. október 25-én aláírt Egyezményt,

az alábbiakban állapodnak meg:

1. CIKK
FOGALOMMEGHATÁROZÁSOK

(1) Jelen Egyezmény alkalmazásában:

1. „Minősített adat”
   (a) a Németországi Szövetségi Köztársaságban:
   megjelenési formájától függetlenül minden közérdekből titokban tartandó tény, adat vagy hír. Ezen adatok minősítése a szükséges védettséggel összhangban valamely hivatalos szerv által vagy javaslatára történik;

   (b) Magyarországon:
   a minősítéssel védhető közérdekek körébe tartozó, a minősítési jelölést a minősített adat védelméről szóló 2009. évi CLV. törvény felhatalmazása alapján kiadott jogszabályokban meghatározott formai követelményeknek megfelelően tartalmazó olyan adat, amelyről - annak megjelenési formájától függetlenül - a minősítő a minősítési eljárás során megállapította, hogy az érvényességi időn belüli nyilvánosságra hozatala, jogosulatlan megszerzése, módosítása vagy felhasználása, illetéktelen személy részére hozzáférhetővé, valamint az arra jogosult részére hozzáférhetetlenné tétele a minősítéssel védhető közérdekek közül bármelyiket közvetlenül sérti vagy veszélyezteti, és tartalmára tekintettel annak nyilvánosságát és megismerhetőségét a minősítés keretében korlátozza.

2. „Minősített szerződés”
   az egyik Szerződő Fél országának valamely hatósága vagy egyéb jogi személye (megrendelő) és a másik Szerződő Fél országának valamely jogi személye (szerződést teljesítő) között létrejött szerződés; amely szerződés alapján a megrendelő az országából származó minősített adatot a szerződést teljesítőnek átadja, aki ezáltal azt felhasználhatja vagy hozzáférhetővé teheti olyan munkatársai számára, akik a megrendelő telephelyén a minősített szerződéssel kapcsolatos feladatot látnak el;
   (a) a megrendelő a minősített szerződésre vonatkozó pályázatot kiíró jogi személy;

(b) a szerződést teljesítő a pályázatot elnyerő és a minősített szerződést végrehajtó jogi személy.

3. „Harmadik fél”
bármely állam, beleértve a joghatósága alá tartozó jogi személyeket vagy természetes személyeket, vagy nemzetközi szervezet, ami nem részese jelen Egyezménynek.

(2) Az egyes minősítési szintek meghatározása a következő:

1. A Németországi Szövetségi Köztársaságban a minősített adat

(a) STRENG GEHEIM, ha az adat jogosulatlan személyek általi megismerése a Németországi Szövetségi Köztársaság vagy valamely szövetségi államának (tartományának) fennállását vagy alapvető érdekét veszélyeztetheti;

(b) GEHEIM, ha az adat jogosulatlan személyek általi megismerése a Németországi Szövetségi Köztársaság vagy valamelyik szövetségi államának (tartományának) biztonságát veszélyeztetheti vagy valamely érdekét súlyosan sértheti;

(c) VS-VERTRAULICH, ha az adat jogosulatlan személyek általi megismerése a Németországi Szövetségi Köztársaság vagy valamelyik szövetségi államának (tartományának) érdekét sértheti;

(d) VS-NUR FÜR DEN DIENSTGEBRAUCH, ha az adat jogosulatlan személyek általi megismerése a Németországi Szövetségi Köztársaság vagy valamelyik szövetségi államának (tartományának) érdekét hátrányosan érintheti.

2. Magyarországon a minősített adat

(a) „Szigorúan titkos!”, ha annak nyilvánosságra hozatala, jogosulatlan megszerzése, módosítása vagy felhasználása, illetéktelen személy részére hozzáférhetővé, valamint az arra jogosult részére hozzáférhetetlenné tétele a minősítéssel védhető közérdeket rendkívül súlyosan károsítja;

(b) „Titkos!”, ha annak nyilvánosságra hozatala, jogosulatlan megszerzése, módosítása vagy felhasználása, illetéktelen személy részére hozzáférhetővé, valamint az arra jogosult részére hozzáférhetetlenné tétele a minősítéssel védhető közérdeket súlyosan károsítja;

(c) „Bizalmas!”, ha annak nyilvánosságra hozatala, jogosulatlan megszerzése, módosítása vagy felhasználása, illetéktelen személy részére hozzáférhetővé, valamint az arra jogosult részére hozzáférhetetlenné tétele a minősítéssel védhető közérdeket károsítja;

(d) „Korlátozott terjesztésű!”, ha annak nyilvánosságra hozatala, jogosulatlan megszerzése, módosítása vagy felhasználása, illetéktelen személy részére hozzáférhetővé, valamint az arra jogosult részére hoz-

záférhetetlenné tétele a minősítéssel védhető közérdeket hátrányosan érinti.

2. CIKK
MEGFELELTETÉS

A Szerződő Felek kijelentik, hogy a minősítések az alábbiak szerint feleltethetők meg egymásnak:

Magyarország	Németországi Szövetségi Köztársaság
„Szigorúan titkos!”	STRENG GEHEIM
„Titkos!”	GEHEIM
„Bizalmas!”	VS-VERTRAULICH
„Korlátozott terjesztésű!”	VS-NUR FÜR DEN DIENSTGEBRAUCH

3. CIKK
JELÖLÉS

(1)Az átadott minősített adatot az átvevő hatáskörrel rendelkező hatósága által vagy ennek a hatóságnak a kezdeményezésére a 2. cikkben szereplő, egymásnak megfeleltethető nemzeti minősítéssel kell jelölni.

(2) Azt a minősített adatot, amely a minősített szerződés kapcsán az átvevő Szerződő Fél országában jött létre, szintén minősítéssel kell jelölni.

(3) Az átadó Szerződő Fél hatáskörrel rendelkező hatóságának kérelmére a minősítést az átvevő hatáskörrel rendelkező hatósága által vagy annak kezdeményezésére meg kell változtatni vagy vissza kell vonni. A minősítés módosításáról vagy visszavonásáról az átadó Szerződő Fél hatáskörrel rendelkező hatósága köteles az másik Szerződő Fél hatáskörrel rendelkező hatóságát haladéktalanul értesíteni.

4. CIKK
NEMZETI SZINTŰ INTÉZKEDÉSEK

(1) A Szerződő Felek nemzeti jogszabályaik alapján megtesznek minden olyan intézkedést, amely biztosítja a jelen Egyezmény hatálya alatt keletkezett, kicserélt vagy tárolt minősített adat védelmét. Ilyen minősített adatoknak legalább olyan szintű védelmet biztosítanak, amelyet az átvevő Szerződő Fél saját, megfeleltethető minősítési szintű minősített adatai esetén megkövetel.

(2) Minősített adat kizárólag a rendeltetése szerinti célra használható fel. A minősített adatot az átvevő Szerződő Fél kizárólag az átadó Szerződő Fél által vagy érdekében meghatározott célokból és korlátozások között teheti közzé, használhatja fel, vagy engedélyezheti közzétételét vagy felhasználását. Minden ettől eltérő intézkedéshez a minősített adat minősítőjének írásos engedélye szükséges.

(3)Minősített adatok kizárólag azon személyek számára tehetőek hozzáférhetővé, akik olyan feladatot látnak el, amelyhez ezen ismeretek szükségesek, és akik – a „Korlátozott terjesztésű!" / VS-NUR FÜR DEN DIENSTGEBRAUCH minősítési szintű minősített adatot kivéve, ha erre a Szerződő Felek nemzeti jogszabályai és egyéb szabályai lehetőséget biztosítanak – megfelelő módon és formában felhatalmazást kaptak a minősített adatnak megfelelő minősítési szintű adatokhoz való hozzáféréshez. Biztonsági tanúsítvány kizárólag legalább olyan szintű biztonsági ellenőrzés lefolytatása után állítható ki, amely a megfelelő minősítési szintű nemzeti minősített adatokhoz való hozzáféréshez előírt szintű biztonsági ellenőrzések szintjével egyenértékű.

(4)A Szerződő Felek országa állampolgárának a „Bizalmas!" / VS-VERTRAULICH vagy az annál magasabb minősítési szintű minősített adathoz való hozzáféréshez az átadó Szerződő Fél nemzeti biztonsági hatósága/ kijelölt biztonsági hatósága vagy egyéb, hatáskörrel rendelkező nemzeti hatósága által kiadott előzetes felhatalmazás nem szükséges.

(5) A személyi biztonsági tanúsítványt a Szerződő Fél országában állampolgársággal és lakóhellyel rendelkező, és ott a minősített adathoz hozzáférést kérő személy részére az adott ország nemzeti biztonsági hatósága/ kijelölt biztonsági hatósága vagy egyéb, hatáskörrel rendelkező nemzeti hatósága állítja ki. Azonban, ha az egyik Szerződő Fél állampolgára a másik Szerződő Fél országában jogszerűen lakóhellyel rendelkezik és ott biztonsági szempontból érzékeny állásra pályázik, akkor a másik Szerződő Fél hatáskörrel rendelkező hatósága állítja ki a személyi biztonsági tanúsítványt és folytatja le a szükséges külföldi ellenőrzéseket.

(6)Jelen Egyezmény 5. és 6. cikkének hatálya nem terjed ki a „Korlátozott terjesztésű!" / VS-NUR FÜR DEN DIENSTGEBRAUCH szinten minősített adatra.

(7)A Szerződő Felek a saját területükön kötelesek gondoskodni a jelen Egyezmény végrehajtásához szükséges és rendelkezéseinek megfelelő nemzetbiztonsági ellenőrzések lefolytatásáról.

5. CIKK
A MINŐSÍTETT SZERZŐDÉS MEGKÖTÉSE

(1) A minősített szerződés elnyerését megelőzően a megrendelő a hatáskörrel rendelkező hatósága közreműködésével beszerzi a szerződést teljesítő telephely biztonsági tanúsítványát annak hatáskörrel rendelkező hatóságától, annak érdekében, hogy meggyőződjön arról, hogy a leendő szerződést teljesítő az adott ország hatáskörrel rendelkező hatóságának biztonsági felügyelete alá tartozik, továbbá arról, hogy a szerződést teljesítő a szerződéses kötelezettségeinek teljesítéséhez szükséges biztonsági óvintézkedéseket foganatosította. Ha a szerződést teljesítő még nem rendelkezik telephely biztonsági tanúsítvánnyal, ennek érdekében kérelmet lehet benyújtani.

(2)A telephely biztonsági tanúsítványt be kell szerezni akkor is, ha egy jogi személy pályázati ajánlattételre kap felhívást, és a szerződés odaítélése előtt a pályázati eljárás részeként részére minősített adatok kiszolgáltatására kerül sor.

(3)Az (1) és (2) bekezdésben említett esetekben a következő eljárást kell alkalmazni:

1. A telephely biztonsági tanúsítvány kiállítására irányuló azon kérelemnek, amelynek alanya a másik Szerződő Fél országának szerződést teljesítője, tartalmaznia kell a projektre vonatkozó információkat, valamint azt, hogy a szerződést teljesítő várhatóan milyen jellegű,

terjedelmű és minősítési szintű minősített adathoz jut hozzá vagy milyen minősített adatot keletkeztet.
2.A telephely biztonsági tanúsítványnak a szerződést teljesítő teljes nevén, levelezési címén, a biztonsági vezető nevén, a szerződést teljesítő telefon és fax számán, és – ha van ilyen, – e-mail címén túl tartalmaznia kell egy arra irányuló kifejezett tájékoztatást, hogy az adott szerződést teljesítő a nemzeti biztonsági szabályok alapján milyen mértékű és milyen minősítési szintű biztonsági rendelkezéseket léptetett életbe.
3.A Szerződő Felek hatáskörrel rendelkező hatóságai kötelesek tájékoztatni egymást a kiállított telephely biztonsági tanúsítványokban foglalt tényekben bekövetkezett bármiféle változásról.
4.Ezen információkról a Szerződő Felek hatáskörrel rendelkező hatóságai angol nyelven tájékoztatják egymást.
5.A telephely biztonsági tanúsítványokat, valamint a telephely biztonsági tanúsítvány kiállítása tárgyában a Szerződő Felek hatáskörrel rendelkező hatóságához címzett kérelmeket írásban kell továbbítani.

6. CIKK
A MINŐSÍTETT SZERZŐDÉSEK TELJESÍTÉSE

(1) A minősített szerződések kötelező tartalmi eleme a biztonsági követelményekről szóló záradék (például biztonsági melléklet), amelyben a szerződést teljesítő kötelezettséget vállal arra, hogy a minősített adatok védelméhez szükséges intézkedéseket a saját országában érvényes nemzeti biztonsági szabályoknak megfelelően foganatosítja.

(2) A biztonsági követelményekről szóló záradék tartalmazza továbbá az alábbi rendelkezéseket:

1. a „minősített adat” fogalmának, valamint a két Szerződő Fél, a jelen Egyezmény rendelkezései szerint egymással megfeleltethető minősítési szintjeinek meghatározását;
2. mindkét Szerződő Fél részéről annak a hatáskörrel rendelkező hatóságnak a megnevezését, amely a szerződésre vonatkozó minősített adatok átadását engedélyezni és azok védelmét koordinálni jogosult;
3. a hatáskörrel rendelkező hatóságok és az érintett szerződést teljesítők között a minősített adatok továbbítására szolgáló csatornákat;
4. a minősített adatok kapcsán, azok minősítésének megváltozása vagy a minősítés szükségességének megszűnése következtében beálló esetleges változásokról történő értesítés folyamatát és módját;
5. a szerződést teljesítők alkalmazottainak látogatását vagy hozzáférését engedélyező eljárást;
6. a minősített adatok olyan szerződést teljesítők felé való továbbítása esetén használatos eljárást, amelyeknél minősített adat kerül felhasználásra vagy tárolásra;
7. azon előírást, amely szerint a szerződést teljesítő a minősített adatokat kizárólag olyan személy számára teheti hozzáférhetővé, akinek a feladatai ellátáshoz ezen ismeretek szükségesek, és aki a szerződés teljesítéséért felel, vagy abban közreműködik, továbbá aki – a „Korlátozott terjesztésű!” / VS-NUR FÜR DEN DIENSTGEBRAUCH jelöléssel ellátott minősített adatot kivéve – megfelelő szintű biztonsági ellenőrzésen átesett;
8. azon előírást, amely szerint harmadik fél részére minősített adatot átadni, vagy az adathoz történő hozzáférést engedélyezni csak akkor lehet, ha ehhez az átadó Szerződő Fél hozzájárult;

9. azon előírást, amely szerint a szerződést teljesítő köteles haladéktalanul értesíteni a hatáskörrel rendelkező hatóságát, ha a szerződés tárgyát képező minősített adat elveszett, kiszivárgott vagy jogosulatlanul került nyilvánosságra, vagy ha ezek gyanúja felmerült.

(3) A megrendelő hatáskörrel rendelkező hatósága köteles a szerződést teljesítőt különálló lista (minősítési útmutató) átadásával tájékoztatni a minősítést igénylő összes adatról, meg kell határoznia a minősítés szükséges szintjét, és biztosítania kell a lista mellékletben történő csatolását a minősített szerződéshez. A megrendelő hatáskörrel rendelkező hatósága köteles továbbá a listát a szerződést teljesítő hatáskörrel rendelkező hatóságához továbbítani, vagy a továbbításról intézkedni.

(4) A megrendelő hatáskörrel rendelkező hatósága köteles gondoskodni arról, hogy a szerződést teljesítő a minősített adatokhoz csak akkor férhessen hozzá, ha a megrendelő hatáskörrel rendelkező hatósága megkapta a szerződést teljesítő hatáskörrel rendelkező hatóságától a vonatkozó telephely biztonsági tanúsítványt.

7. CIKK
A MINŐSÍTETT ADAT TOVÁBBÍTÁSA

(1) A „Szigorúan titkos!” / STRENG GEHEIM minősítési szintű minősített adatot a Szerződő Felek kizárólag diplomáciai úton, a nemzeti biztonsági szabályaikban meghatározottak szerint továbbíthatják egymásnak.

(2) Főszabályként a „Bizalmas!” / VS-VERTRAULICH és a „Titkos!” / GEHEIM minősítési szintű minősített adatot a nemzeti jogszabályokkal és egyéb szabályokkal összhangban hivatalos futár továbbítja az egyik országból a másikba. A Szerződő Felek nemzeti biztonsági hatóságai/ kijelölt biztonsági hatóságai egyéb továbbítási mód használatában is megállapodhatnak. A minősített adat átvételének visszaigazolása a hatáskörrel rendelkező hatóság által vagy javaslatára történik, és a minősített adatot a nemzeti biztonsági szabályoknak megfelelően kell az átvevőnek továbbítani.

(3) A hatáskörrel rendelkező hatóságok, az általuk közösen meghatározott projektek esetén megállapodhatnak abban, hogy a „Bizalmas!” / VS-VERTRAULICH és a „Titkos!” / GEHEIM minősítési szintű minősített adatot általános jelleggel vagy bizonyos korlátozásokkal a hivatalos futárszolgálattól eltérő úton is lehet továbbítani, ha a hivatalos futárszolgálat igénybevétele az adat továbbítását vagy a szerződés végrehajtását szükségtelenül megnehezítené. Ezekben az esetekben:

1. az adatot szállító személynek olyan szintű felhatalmazással kell rendelkeznie, amely a minősített adat minősítési szintjének megfelelő szintű minősített adathoz való hozzáférésre jogosítja;
2. a küldő szervezet köteles a továbbított adatok tételes listáját megőrizni; e tételes lista egy másolati példányát a hatáskörrel rendelkező hatóság részére történő továbbítás céljából át kell adni az átvevőnek;
3. a minősített adat egyes tételeit az országhatáron belüli szállításra vonatkozó szabályok szerint kell csomagolással ellátni;
4. a minősített adat egyes tételeit átvételi elismervény ellenében kell kézbesíteni;
5. a minősített adatot szállító személynek a feladó hatáskörrel rendelkező hatósága vagy a címzett hatáskörrel rendelkező hatósága által kiállított futárigazolvánnyal kell rendelkeznie.

(4) Nagy mennyiségű minősített adat továbbítása esetén a szállítóeszközt, az útvonalat és a kísérő személyzet összetételét a hatáskörrel rendelkező hatóságok esetről esetre, részletes szállítási terv alapján határozzák meg.

(5) A „Bizalmas!" / VS-VERTRAULICH és magasabb minősítési szintű minősített adat elektronikus továbbítása kizárólag rejtjelezve történik. Az ilyen minősítési szintű minősített adatokat kizárólag a Szerződő Felek hatáskörrel rendelkező biztonsági hatóságai által kölcsönös megegyezésben jóváhagyott rejtjelző eszközzel lehet titkosítani.

(6) A „Korlátozott terjesztésű!" / VS-NUR FÜR DEN DIENSTGEBRAUCH minősítési szintű minősített adatot a másik Szerződő Fél területén található címzettnek postai úton vagy egyéb kézbesítő szolgálat igénybevételével a nemzeti biztonsági szabályok figyelembevételével lehet továbbítani.

(7) A „Korlátozott terjesztésű!" / VS-NUR FÜR DEN DIENSTGEBRAUCH minősítési szintű minősített adat elektronikus úton is továbbítható vagy elérhetővé tehető a kereskedelmi forgalomban kapható és a Szerződő Felek hatáskörrel rendelkező nemzeti hatósága által jóváhagyott kereskedelmi rejtjelző eszközön keresztül. E minősítési szintű minősített adatokat rejtjelzés nélkül csak akkor lehet továbbítani, ha az nem ellentétes az erre vonatkozó nemzeti biztonsági szabályokkal, ha jóváhagyott rejtjelző eszköz nem áll rendelkezésre, ha a továbbítás kizárólag fix telepítésű hálózatokon történik, valamint ha a feladó és a címzett a kilátásba helyezett továbbításról előzetesen megállapodott.

8. CIKK
A MINŐSÍTETT ADAT SOKSZOROSÍTÁSA, FORDÍTÁSA ÉS MEGSEMMISÍTÉSE

(1)A jelen Egyezmény alapján átadott 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 mennyiségre kell korlátozni.

(2) A jelen Egyezmény alapján átadott minősített adat fordítása során keletkező példányokon a fordítás nyelvén fel kell tüntetni, hogy az átadó Szerződő Fél minősített adatát tartalmazzák.

(3) A jelen Egyezmény alapján átadott, „Szigorúan titkos!" / STRENG GEHEIM minősítési szintű minősített adat fordítása vagy sokszorosítása kizárólag az átadó Szerződő Fél előzetes írásbeli engedélyével lehetséges.

(4) A jelen Egyezmény alapján átadott, „Szigorúan titkos!" / STRENG GEHEIM minősítési szintű minősített adat nem semmisíthető meg, e minősítési szintű minősített adatokat az átadó Szerződő Félnek vissza kell szolgáltatni.

9. CIKK
LÁTOGATÁSOK

(1) Főszabályként az egyik Szerződő Fél területéről érkező látogató részére a másik Szerződő Fél területén kizárólag a meglátogatni kívánt Szerződő Fél országa hatáskörrel rendelkező hatóságának előzetes engedélyével biztosítható hozzáférés minősített adathoz, valamint minősített adat kezelését végző létesítményhez. Engedélyt kizárólag olyan személyek kaphatnak, akiknek feladataik ellátásához szükséges a minősített adatok megismerése, és akik – a „Korlátozott terjesztésű!" / VS-NUR FÜR DEN DIENSTGEBRAUCH jelöléssel ellátott minősített adatot kivéve, ha erre a Szerződő Felek nemzeti jogszabályai és egyéb szabályai lehetőséget biztosítanak – felhatalmazással rendelkeznek minősített adathoz való hozzáférésre.

(2) A látogatás iránti kérelmet megfelelő időben, annak a Szerződő Félnek a szabályai szerint kell a Szerződő Fél hatáskörrel rendelkező hatóságához benyújtani, amelynek területére a látogató be kíván lépni. A hatáskörrel rendelkező hatóságok tájékoztatják egymást a kérelmek részleteiről, és gondoskodnak a személyes adatok védelméről.

(3) A látogatás iránti kérelmet a látogatás célországának nyelvén vagy angol nyelven kell benyújtani az alábbi tartalommal:

1. a látogató vezeték- és utóneve, születési helye és ideje, személyazonosító igazolványának vagy útlevelének száma;
2. a látogató állampolgársága;
3. a látogató szolgálati beosztása és az általa képviselt hatóságnak vagy szervezetnek a megnevezése;
4. a látogatót a minősített adatokhoz való hozzáférésre feljogosító személyi biztonsági tanúsítvány szintje;
5. a látogatás célja, továbbá, amennyiben lehetséges, a látogatással érintett legmagasabb minősítési szintű minősített adat minősítési szintje, valamint a látogatás tervezett időpontja és időtartama;
6. a meglátogatni kívánt létesítmény megnevezése és címe, valamint a kapcsolattartó neve, telefon/fax száma és e-mail címe;
7. dátum, aláírás és a hatáskörrel rendelkező hatóság hivatalos bélyegzőlenyomata.

(4)A hatáskörrel rendelkező hatóságok közösen meghatározhatják a visszatérő látogatásra jogosultak listáját. A visszatérő látogatások további részleteit a hatáskörrel rendelkező hatóságok közösen állapítják meg. A látogató által megismert minősített adatot a jelen Egyezmény alapján átvett minősített adatnak kell tekinteni.

10. CIKK
KONZULTÁCIÓ

(1) A Szerződő Felek hatáskörrel rendelkező hatóságai figyelembe veszik a minősített adatok védelmére vonatkozóan a másik Szerződő Fél területén érvényes rendelkezéseket.

(2) A jelen Egyezmény végrehajtásához szükséges szoros együttműködés érdekében a hatáskörrel rendelkező hatóságok konzultációt tartanak, ha azt valamelyik hatóság kéri.

(3) Ezen túlmenően a Szerződő Felek biztosítják, hogy területükön a másik Szerződő Fél nemzeti biztonsági hatósága/ kijelölt biztonsági hatósága vagy kölcsönös megállapodásban kijelölt egyéb hatósága látogatást tehessen a biztonsági hatóságokkal a másik Szerződő Féltől

kapott minősített adatok védelmét biztosító eljárásokról és létesítményekről szóló konzultáció folytatása érdekében. Mindkét Szerződő Fél támogatást nyújt az adott hatóságnak annak megállapításához, hogy a másik Szerződő Fél által rendelkezésre bocsátott minősített adat megfelelő védelemben részesül-e. A látogatás részleteit a hatáskörrel rendelkező hatóságok rögzítik.

11. CIKK
A MINŐSÍTETT ADAT KÖLCSÖNÖS VÉDELMÉRE VONATKOZÓ RENDELKEZÉSEK MEGSÉRTÉSE

(1) Ha a minősített adat jogosulatlan nyilvánosságra hozatala nem zárható ki, vagy ennek gyanúja felmerül, vagy ténye megállapítást nyer, a másik Szerződő Felet haladéktalanul írásban tájékoztatni kell a biztonság megsértésének körülményeiről, a kár mértékéről, a kárenyhítés érdekében megtett intézkedésekről, valamint a vizsgálat eredményéről a nemzeti jogszabályok és egyéb szabályok rendelkezéseivel összhangban.

(2)A minősített adatok védelmét előíró rendelkezések megsértését ki kell vizsgálni, és a joghatósággal rendelkező Szerződő Fél hatáskörrel rendelkező hatóságai és bíróságai kötelesek megtenni e Szerződő Fél jogszabályainak megfelelő jogi lépéseket. A másik Szerződő Fél erre vonatkozó megkeresés esetén az ilyen vizsgálathoz segítséget nyújt, annak eredményéről tájékoztatást kap.

12. CIKK
KÖLTSÉGEK VISELÉSE

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

13. CIKK
JOGVITÁK RENDEZÉSE

A Szerződő Felek a jelen Egyezmény értelmezése vagy alkalmazása tárgyában közöttük felmerülő bármely vitát tárgyalások útján egymás között rendezik, azt rendezésre sem nemzeti, sem nemzetközi bíróság, sem egyéb harmadik fél elé nem utalhatják.

14. CIKK
HATÁSKÖRREL RENDELKEZŐ HATÓSÁGOK

A Szerződő Felek tájékoztatják egymást a jelen Egyezmény végrehajtásáért felelős hatóságaikról.

15. CIKK
KAPCSOLAT MÁS EGYEZMÉNYEKKEL, EGYETÉRTÉSI NYILATKOZATOKKAL ÉS MEGÁLLAPODÁSOKKAL

Jelen Egyezmény nincs kihatással a Szerződő Felek vagy a hatáskörrel rendelkező hatóságok között fennálló egyéb minősített adatok védelmével foglalkozó egyezményekre, egyetértési nyilatkozatokra és megállapodásokra, amennyiben azok nem állnak ellentmondásban jelen Egyezmény rendelkezéseivel.

16. CIKK
ZÁRÓ RENDELKEZÉSEK

(1) Jelen Egyezmény azon jegyzék kézhezvételét követő 30. napon lép hatályba, amellyel Magyarország Kormánya értesíti a Németországi Szövetségi Köztársaság Kormányát arról, hogy a hatályba lépés nemzeti feltételei teljesültek.

(2) Jelen Egyezmény határozatlan időre jön létre.

(3) Jelen Egyezmény a Szerződő Felek kölcsönös egyetértésével írásban módosítható. Jelen Egyezmény módosítását írásos beadványban bármelyik Szerződő Fél bármikor kérelmezheti. Ha valamelyik Szerződő Fél ilyen megkereséssel fordul a másik Szerződő Félhez, a Szerződő Felek kötelesek a jelen Egyezmény módosításáról tárgyalásokat kezdeni.

(4) Bármelyik Szerződő Félnek jogában áll jelen Egyezményt diplomáciai úton hathónapos határidővel írásban felmondani. Felmondás esetén a szerződést teljesítő által továbbított vagy létrehozott minősített adatot jelen Egyezmény alapján továbbra is a jelen Egyezmény 4. cikke rendelkezései szerint kell kezelni, amíg a minősítés fenntartása indokolt.

(5) Jelen Egyezménynek az Egyesült Nemzetek Alapokmányának 102. cikke szerinti nyilvántartásba vételét az Egyesült Nemzetek Titkárságánál közvetlenül a hatálybalépést követően az a Szerződő Fél köteles kezdeményezni, amelynek a területén jelen Egyezményt megkötik. A másik Szerződő Felet a nyilvántartásba vételről és az ENSZ nyilvántartási számról közvetlenül a Titkárságtól kapott visszaigazolást követően tájékoztatni kell.

(6) Jelen Egyezmény hatálybalépésével hatályát veszti a Magyar Köztársaság Kormánya és a Németországi Szövetségi Köztársaság Kormánya között a minősített információk kölcsönös védelme tárgyában 1995. október 25-én aláírt Egyezmény.

Kelt Budapesten, 2018. 08. 23. napján két eredeti példányban magyar, német és angol nyelven, mindhárom nyelvi változat hiteles. A magyar és a német nyelvi változat eltérő értelmezése esetén az angol nyelvi változat tekintendő irányadónak.

Magyarország Kormánya részéről

A Németországi Szövetségi Köztársaság Kormánya részéről”

„AGREEMENT

BETWEEN

THE GOVERNMENT OF HUNGARY

AND

THE GOVERNMENT OF THE FEDERAL REPUBLIC OF GERMANY

ON THE

MUTUAL PROTECTION OF CLASSIFIED INFORMATION

The Government of Hungary
and
the Government of the Federal Republic of Germany,
(hereinafter referred to as "the Contracting Parties"),

Intending to ensure the protection of classified information that is exchanged between the competent authorities of Hungary and the Federal Republic of Germany as well as with contractors in the territory of the other Contracting Party or between contractors of the two Contracting Parties,

Desirous of laying down an arrangement on the mutual protection of classified information that shall apply to all agreements on cooperation to be concluded between the Contracting Parties and to contracts involving an exchange of classified information,

Wishing to replace the Agreement between the Government of the Republic of Hungary and the Government of the Federal Republic of Germany on the Mutual Protection of Classified Information of 25th of October 1995 with a new version,

Have agreed as follows:

ARTICLE 1
DEFINITIONS

(1) For the purposes of this Agreement

1. classified information is

   (a) in the Federal Republic of Germany
   facts, items or intelligence which, regardless of how they are presented, are to be kept secret in the public interest. They shall be classified by, or at the instance of, an official agency in accordance with their need for protection;

   (b) in Hungary
   information within the scope of public interest to be protected by classification, fulfilling the formal requirements of regulations issued under the Act CLV of 2009 on the Protection of Classified Information and marked for classification through this Act, for which – irrespective of its form – the originator defined through the classification process that within the term of validity, any kind of disclosure, unauthorised access, amendment or usage, providing access for unauthorised persons or blocking the access of authorised persons can directly harm or jeopardise public interests to be protected by classification and will limit its disclosure and access to its contents through classification.

2. a classified contract is

   a contract between an authority or another legal entity from the country of one Contracting Party (contracting officer) and a legal entity from the country of the other Contracting Party (contractor); under such contract, classified information from the country of the contracting officer is to be released to the contractor, is to be developed by the contractor or is to be made accessible to members of the contractor's staff who are to perform tasks in facilities of the contracting officer.

   (a) A contracting officer is a legal entity which grants a classified contract.
   (b) A contractor is a legal entity which receives and executes a classified contract.

3. a third party is
   any country including legal entities or individuals under its jurisdiction or international organisation not being a party to this Agreement.

(2) The levels of security classification are defined as follows:

1. In the Federal Republic of Germany, classified information is

   (a) STRENG GEHEIM if knowledge of it by unauthorised persons may pose a threat to the existence or vital interests of the Federal Republic of Germany or one of its states *(Länder)*,
   (b) GEHEIM if knowledge of it by unauthorised persons may pose a threat to the security of the Federal Republic of Germany or one of its states *(Länder)*, or may cause severe damage to their interests,
   (c) VS-VERTRAULICH if knowledge of it by unauthorised persons may be damaging to the interests of the Federal Republic of Germany or one of its states *(Länder)*,
   (d) VS-NUR FÜR DEN DIENSTGEBRAUCH if knowledge of it by unauthorised persons may be disadvantageous to the interests of the Federal Republic of Germany or one of its states *(Länder)*.

2. In Hungary, classified information is

   (a) "Szigorúan titkos!" in case the disclosure of, unauthorised access to, amendment or use of the information, granting access to unauthorised persons or denying access to authorised persons shall cause extremely severe damage to public interests to be protected by classification,
   (b) "Titkos!" in case the disclosure of, unauthorised access to, amendment or use of the information, granting access to unauthorised persons or denying access to authorised persons shall cause severe damage to public interests to be protected by classification,
   (c) "Bizalmas!" in case the disclosure of, unauthorised access to, amendment or use of the information, granting access to unauthorised persons or denying access to authorised persons shall cause damage to public interests to be protected by classification,
   (d) "Korlátozott terjesztésű!" in case the disclosure of, unauthorised access to, amendment or use of the information, granting access to unauthorised persons or deny-

ing access to authorised persons shall negatively affect public interests to be protected by classification.

ARTICLE 2
COMPARABILITY

The Contracting Parties stipulate that the following security classifications shall be comparable:

For Hungary	For the Federal Republic of Germany
"Szigorúan titkos!"	STRENG GEHEIM
"Titkos!"	GEHEIM
"Bizalmas!"	VS-VERTRAULICH
"Korlátozott terjesztésű!"	VS-NUR FÜR DEN DIENSTGEBRAUCH

ARTICLE 3
MARKING

(1) Transmitted classified information shall be marked with the comparable national security classification as provided under Article 2 by, or at the instance of, the competent authority of the recipient.

(2) Classified information which is generated in the receiving country in connection with classified contracts shall also be marked.

(3) Security classifications shall, at the request of the competent authority of the originating Contracting Party, be amended or revoked by, or at the instance of, the competent authority of the recipient of the given classified information. The competent authority of the originating Contracting Party shall immediately inform the competent authority of the other Contracting Party of amendments or revocations of a security classification.

ARTICLE 4
MEASURES AT THE NATIONAL LEVEL

(1) Within the scope of their national legislation, the Contracting Parties shall take all appro-

priate measures to guarantee the security protection of classified information generated, exchanged or held under the terms of this Agreement. They shall afford such classified information a degree of security protection at least equal to that required by the receiving Contracting Party for its own classified information of the comparable level of security classification.

(2) The classified information shall be used solely for the designated purpose. The receiving Contracting Party shall not disclose or use, or permit the disclosure or use of, any classified information except for the purposes and within any limitations stated by or on behalf of the originating Contracting Party. The originator of the classified information must have given his written consent to any arrangement to the contrary.

(3) In accordance with the national laws and regulations of the Contracting Parties, access to classified information may be granted only to persons having a need-to-know on account of their duties and – except in the case of classified information at the "Korlátozott terjesztésű!" / VS-NUR FÜR DEN DIENSTGEBRAUCH level – having been authorised to have access to classified information of the comparable level of security classification. Security clearance shall be granted only after completion of security screening under standards no less stringent than those applied for access to national classified information of the comparable level of security classification.

(4) Access to classified information at the "Bizalmas!" / VS-VERTRAULICH level or higher by a person holding the nationality of a Contracting Party shall be granted without prior authorisation of the National Security Authority / Designated Security Authority or other competent national authorities of the originating Contracting Party.

(5) Personal Security Clearances for nationals of the Contracting Party residing, and requiring access to classified information, in their own country shall be undertaken by their National Security Authorities / Designated Security Authorities or other competent national authorities. However, Personal Security Clearances for nationals of one Contracting Party who are legally resident in the country of the other Contracting Party and apply for a security-sensitive job in that country shall be undertaken by the competent security authority of that country, conducting overseas checks as appropriate.

(6) Article 5 and Article 6 of this Agreement shall not apply to classified information at the

"Korlátozott terjesztésű!" / VS-NUR FÜR DEN DIENSTGEBRAUCH level.

(7) The Contracting Parties shall, each within its territory, ensure that the security inspections necessary for the implementation of this Agreement are carried out and that this Agreement is complied with.

ARTICLE 5
AWARD OF CLASSIFIED CONTRACTS

(1) Prior to the award of a classified contract, the contracting officer shall, through its competent authority, obtain a Facility Security Clearance from the competent authority of the contractor in order to obtain assurance as to whether the prospective contractor is subject to security oversight by the competent authority of this country and whether it has taken the security precautions required for discharging the performance of the contract. Where a contractor has not yet been granted a Facility Security Clearance, an application may be made to that end.

(2) A Facility Security Clearance shall also be obtained if a legal entity has been requested to submit a bid and if classified information will have to be released prior to the award of a contract under the bid procedure.

(3) In the cases referred to in paragraphs (1) and (2) above, the following procedure shall be applied:

1. Requests for the issuance of a Facility Security Clearance for contractors from the country of the other Contracting Party shall contain information on the project as well as the nature, the scope and the level of security classification of the classified information expected to be released to the contractor or to be generated by it.
2. In addition to the full name of the contractor, its postal address, the name of its security official, its telephone and fax number and, if applicable, its e-mail address, Facility Security Clearances must include information in particular on the extent to which, and the level of security classification up to which, security measures have been taken by the respective contractor on the basis of national security regulations.
3. The competent authorities of the Contracting Parties shall inform each other of any

changes in the facts covered by issued Facility Security Clearances.

4. The exchange of such information between the competent authorities of the Contracting Parties shall be effected in English.
5. Facility Security Clearances and requests addressed to the respective competent authorities of the Contracting Parties for the issuance of Facility Security Clearances shall be transmitted in written form.

ARTICLE 6
PERFORMANCE OF CLASSIFIED CONTRACTS

(1) Classified contracts must contain a security requirement clause (e.g. Security Aspects Letter) under which the contractor is under an obligation to make the arrangements required for the protection of classified information pursuant to the national security regulations of its country.

(2) In addition, the security requirement clause shall contain the following provisions:

1. the definition of the term "classified information" and of the comparable levels of security classification of the two Contracting Parties in accordance with the provisions of this Agreement;
2. the names of the competent authority of each of the two Contracting Parties empowered to authorise the release and to coordinate the safeguarding of classified information related to the contract;
3. the channels to be used for the transfer of classified information between the competent authorities and contractors involved;
4. the procedures and mechanisms for communicating changes that may arise in respect of classified information either because of changes in its security classification or because classification is no longer necessary;
5. the procedures for the approval of visits, or access, by personnel of the contractors;
6. the procedures for transmitting classified information to contractors where such information is to be used or held;
7. the requirement that the contractor shall grant access to classified information only to a person who has a need-to-know and has been charged with, or contributes to, the performance of the contract and – except in the case of classified information at the

"Korlátozott terjesztésű!" / VS-NUR FÜR DEN DIENSTGEBRAUCH level – has been security-cleared to the appropriate level in advance;

8. the requirement that classified information shall only be disclosed, or the disclosure of classified information shall only be permitted, to a third party if this has been approved by the originating Contracting Party;
9. the requirement that the contractor shall immediately notify his competent authority of any actual or suspected loss, leak or unauthorised disclosure of the classified information covered by the contract.

(3) The competent authority of the contracting officer shall provide the contractor with a separate list (classification guide) of all documentary records requiring security classification, shall determine the required level of security classification and shall arrange for this list to be enclosed as an appendix to the classified contract. The competent authority of the contracting officer shall also transmit, or arrange for the transmission of, the list to the competent authority of the contractor.

(4) The competent authority of the contracting officer shall ensure that the contractor will be given access to classified information only after the pertinent Facility Security Clearance has been received from the competent authority of the contractor.

ARTICLE 7
TRANSMISSION OF CLASSIFIED INFORMATION

(1) Classified information at the "Szigorúan titkos!" / STRENG GEHEIM level shall only be transmitted between the Contracting Parties through diplomatic channels pursuant to the national security regulations.

(2) As a matter of principle, classified information at the "Bizalmas!" / VS-VERTRAULICH and "Titkos!" / GEHEIM levels shall be transmitted from one country to another by official courier in accordance with the national laws and regulations. The National Security Authorities / Designated Security Authorities of the Contracting Parties may agree on alternative channels of transmission. Receipt of classified information shall be confirmed by, or at the instance of, the competent authority and the classified information shall be forwarded to the recipient in accordance with national security regulations.

(3) For a specifically designated project, the competent authorities may agree – generally or subject to restrictions – that classified information at the "Bizalmas!" / VS-VERTRAULICH and "Titkos!" / GEHEIM levels may be transmitted through channels other than official courier if reliance on the official courier service would cause undue difficulties for such transportation or for the execution of a contract. In such cases

1. the bearer must be authorised to have access to classified information of the comparable level of security classification;
2. a list of the items of classified information transmitted must be retained by the dispatching agency; a copy of this list shall be handed over to the recipient for forwarding to the competent authority;
3. items of classified information must be packed in accordance with the regulations governing transportation within national boundaries;
4. items of classified information must be delivered against receipt;
5. the bearer must carry a courier certificate issued by the competent authority of the dispatching or the receiving agency.

(4) Where large volumes of classified information are to be transmitted, the means of transportation, the route, and the escort shall be determined on a case-by-case basis and on the basis of a detailed transport plan by the competent authorities.

(5) The electronic transmission of classified information at the "Bizalmas!" / VS-VERTRAULICH level and higher must not take place in an unencrypted form. Classified information of these levels of security classification may only be encrypted by encryption means approved by mutual agreement by the competent security authorities of the Contracting Parties.

(6) Classified information at the "Korlátozott terjesztésű!" / VS-NUR FÜR DEN DIENSTGEBRAUCH level may be transmitted by post or other delivery services to recipients within the territory of the other Contracting Party, taking into account national security regulations.

(7) Classified information at the "Korlátozott terjesztésű!" / VS-NUR FÜR DEN DIENSTGEBRAUCH level may be electronically transmitted or made available by means of commercial encryption devices approved by a competent national authority of the Contracting Parties.

Classified information of this level of security classification may only be transmitted in an unencrypted form provided that this is not in contradiction with national security regulations, that no approved encryption means are available, transmission is effected within fixed networks only and the sender and the recipient have reached agreement on the proposed transmission in advance.

ARTICLE 8
REPRODUCTION, TRANSLATION AND DESTRUCTION OF CLASSIFIED INFORMATION

(1) Reproductions and translations of classified information released under this Agreement shall bear appropriate security classification markings and shall be protected as the originals. The number of reproductions shall be limited to that required for official purposes.

(2) Translations of classified information released under this Agreement shall bear a note in the language of translation indicating that they contain classified information of the originating Contracting Party.

(3) Classified information released under this Agreement marked "Szigorúan titkos!" / STRENG GEHEIM shall be translated or reproduced only upon the prior written consent of the originating Contracting Party.

(4) Classified information released under this Agreement marked "Szigorúan titkos!" / STRENG GEHEIM shall not be destroyed but shall be returned to the originating Contracting Party.

ARTICLE 9
VISITS

(1) As a matter of principle, it is only with the prior permission of the competent authority of the Contracting Party the country of which is to be visited that visitors from the territory of one Contracting Party will, on the territory of the other Contracting Party, be granted access to classified information and to facilities in which classified information is being handled. In accordance with the national laws and regulations of the Contracting Parties such permission shall be given only to persons having a need-to-know and – except in the case of classified in-

formation at the "Korlátozott terjesztésű!" / VS-NUR FÜR DEN DIENSTGEBRAUCH level – having been authorised to have access to classified information.

(2) Requests for visits shall be submitted, on a timely basis and in accordance with the regulations of the Contracting Party whose territory such visitors wish to enter, to the competent authority of that Contracting Party. The competent authorities shall inform each other of the details regarding such requests and shall ensure that personal data are protected.

(3) Requests for visits shall be submitted in the language of the country to be visited or in English and shall contain the following information:

1. the visitor's first name and surname, date and place of birth, and his/her passport or identity card number;
2. the visitor's nationality;
3. the visitor's service designation, and the name of the authority or agency which the visitor represents;
4. the level of the visitor's security clearance for access to classified information;
5. the purpose of the visit including, if possible, the highest security classification level of classified information involved, and the proposed date and duration of the visit;
6. 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;
7. date, signature and official seal of the competent authority.

(4) The competent authorities may agree on a list of visitors entitled to recurring visits. The competent authorities shall agree on the further details of the recurring visits. Classified information acquired by a visitor shall be considered as classified information received under this Agreement.

ARTICLE 10
CONSULTATIONS

(1) The competent authorities of the Contracting Parties shall take note of the provisions governing the protection of classified information that apply within the territory of the other Contracting Party.

(2) To ensure close cooperation in the implementation of this Agreement, the competent authorities shall consult each other at the request of one of these authorities.

(3) Each Contracting Party shall, in addition, allow the National Security Authority / Designated Security Authority of the other Contracting Party or any other authority designated by mutual agreement to visit its territory in order to discuss, with its security authorities, its procedures and facilities for the protection of classified information received from the other Contracting Party. Each Contracting Party shall assist that authority in ascertaining whether such classified information which has been made available by the other Contracting Party is adequately protected. The details of the visits shall be laid down by the competent authorities.

ARTICLE 11
VIOLATIONS OF PROVISIONS GOVERNING THE MUTUAL PROTECTION OF CLASSIFIED INFORMATION

(1) Whenever unauthorised disclosure of classified information cannot be ruled out or if such disclosure is suspected or ascertained, the other Contracting Party shall immediately be informed 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 in accordance with the national laws and regulations.

(2) Violations of provisions governing the protection of classified information shall be investigated, and pertinent legal action shall be taken, by the competent authorities and courts of the Contracting Party having jurisdiction, according to that Contracting Party's law. The other Contracting Party should, if so requested, support such investigations and shall be informed of the outcome.

ARTICLE 12
COSTS

Each Contracting Party shall pay the expenses incurred by it in implementing the provisions of this Agreement.

ARTICLE 13
DISPUTE SETTLEMENT

Any dispute between the Contracting Parties regarding the interpretation or application of this Agreement shall be resolved by consultation between the Contracting Parties and shall not be referred to any national or international tribunal or third party for settlement.

ARTICLE 14
COMPETENT AUTHORITIES

The Contracting Parties shall inform each other of the authorities to be responsible for the implementation of this Agreement.

ARTICLE 15
RELATIONSHIP WITH OTHER AGREEMENTS, MEMORANDA OF UNDERSTANDING AND ARRANGEMENTS

Any existing Agreements, Memoranda of Understanding and Arrangements between the Contracting Parties or the competent authorities on the protection of classified information shall be unaffected by the present Agreement in so far as they do not conflict with its provisions.

ARTICLE 16
FINAL PROVISIONS

(1) This Agreement shall enter into force 30 days from the date on which the Government of Hungary has notified the Government of the Federal Republic of Germany that the national requirements for such entry into force have been fulfilled. The relevant date shall be the date of receipt of the notification.

(2) This Agreement is concluded for an indefinite period of time.

(3) This Agreement may be amended in writing by mutual agreement between the Contracting Parties. Either Contracting Party may at any time submit a written request for the amendment of this Agreement. If such a request is submitted by one of the Contracting Parties, the Contracting Parties shall initiate negotiations on the amendment of the Agreement.

(4) Either Contracting Party may, through diplomatic channels, denounce this Agreement by giving six months' written notice. In the event of denunciation, classified information transmitted, or generated by the contractor, on the basis of this Agreement shall continue to be treated in accordance with the provisions of Article 4 above for as long as is justified by the existence of the security classification.

(5) Registration of this Agreement with the Secretariat of the United Nations, in accordance with Article 102 of the United Nations Charter, shall be initiated by the Contracting Party on whose national territory the Agreement is concluded immediately following its entry into force. The other Contracting Party shall be informed of registration, and of the UN registration number, as soon as this has been confirmed by the Secretariat.

(6) With the entry into force of this Agreement, the Agreement between the Government of the Republic of Hungary and the Government of the Federal Republic of Germany on the Mutual Protection of Classified Information of 25th of October 1995, shall expire.

Done at Budapest on August 23, 2018 in duplicate in the Hungarian, German and English languages, all three texts being authentic. In case of divergent interpretations of the Hungarian and German texts, the English text shall prevail.

For the Government of Hungary

For the Government of the Federal Republic of Germany"

4. §

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

(2) A 2. § és 3. § az Egyezmény 16. Cikkében 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 Egyezmény hatálybalépésével hatályát veszti 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.

5. §

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

Indokolás a Magyarország Kormánya és a Németországi Szövetségi Köztársaság Kormánya között a minősített adatok kölcsönös védelméről szóló egyezmény kihirdetéséről szóló törvényjavaslathoz

Általános indokolás

A két szerződő fél 1995-ban már kötött egy hasonló témájú megállapodást: a Magyar Köztársaság Kormánya és a Németországi Szövetségi Köztársaság Kormánya között a minősített információk kölcsönös védelme tárgyában, Budapesten, 1995. október 25-én aláírt Egyezmény (a továbbiakban: 1995-ös Egyezmény), amelyet a 1996. évi XXXV. törvény hirdetett ki. Az 1995-ös Egyezmény új, a minősített adatok kölcsönös védelmét szabályozó egyezménnyel való felváltása azért szükséges, mert az Országgyűlés 2009. december 14-én elfogadta a minősített adat védelméről szóló 2009. évi CLV. törvényt (a továbbiakban: Mavtv.), amely alapjaiban kodifikálta újra a minősített adatok védelmének magyarországi struktúráját. Az 1995-ös Egyezmény módosítására tehát a hatálybalépését követően eltelt időszakban bekövetkezett jogszabályi, valamint szervezeti változások miatt van szükség. Az új Egyezmény az 1995-ös Egyezménnyel azonos alapokon nyugszik: az adatokhoz való hozzáférést biztosító szabályok megfelelnek a szükséges ismeret elvének, a felek az Egyezmény keretében átadott adatokat az azonos védelem elve alapján részesítik védelemben, az átadó fél megtartja az átadott adatok feletti rendelkezési jogot (az adatok minősítési szintjét az átvevő fél csak az átadó fél hozzájárulása esetén változtathatja meg, az átadott adatok harmadik félnek csak az átadó fél hozzájárulásával adhatóak tovább).

Az új Egyezmény azonban részletesebb szabályokat tartalmaz többek között a minősített szerződésekre, valamint a felek közötti látogatásokra.

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 „azon a napon lép hatályba, amikor Magyarország Kormánya értesítést küld a Németországi Szövetségi Köztársaság Kormányának arról, hogy a hatályba lépés nemzeti feltételei teljesültek.” Ennek oka, hogy az Egyezmény kötelező hatályának elismerésére a Felek által alkalmazandó alkotmányos vagy belső jogi szabályokkal és eljárásokkal összhangban kerül sor és a német jogi szabályozás szerint az aláírással a hatályba lépés nemzeti feltételei teljesülnek. Az Egyezmény hatálybalépésének naptári napját a külpolitikáért felelős miniszter annak ismertté válását követően a Magyar Közlönyben közzétett egyedi közleményével állapítja meg.
Mivel az Egyezmény 16. cikkének (6) bekezdése hatályon kívül helyezi a felek között 1995-ban aláírt Egyezményt, a kihirdető törvény záró rendelkezései között szükséges rendelkezni az 1995-ös Egyezményt kihirdető törvény hatályon kívül helyezéséről. A törvény hatályon kívül helyezésének napja megegyezik az Egyezmény hatálybalépésének napjával.

az 5. §-hoz

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