MAGYARORSZÁG KORMÁNYA

Átiktatva: T/409.

~~**T/20375. számú**~~

törvényjavaslat

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

1. §

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

2. §

Az Országgyűlés az Egyezményt e törvénnyel kihirdeti.

3. §

Az Egyezmény hiteles magyar és angol nyelvű szövege a következő:

“EGYEZMÉNY MAGYARORSZÁG KORMÁNYA ÉS A LITVÁN KÖZTÁRSASÁG KORMÁNYA KÖZÖTT A MINŐSÍTETT ADATOK CSERÉJÉRŐL ÉS KÖLCSÖNÖS VÉDELMÉRŐL

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

elismerve a kölcsönös politikai, gazdasági és katonai együttműködés fontos szerepét,

felismerve, hogy a Felek közötti jó együttműködés során szükség lehet minősített adatok cseréjére vagy létrehozására,

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

kívánatosnak tartva, hogy a közöttük kicserélt vagy általuk létrehozott minősített adatok megfelelő védelemben részesüljenek,

kölcsönösen tiszteletben tartva a nemzeti érdekeket és a biztonságot, az alábbiakban állapodtak meg:

1. CIKK

AZ EGYEZMÉNY CÉLJA ÉS TÁRGYA

(1) Jelen Egyezmény célja, hogy védelmet biztosítson a Felek közötti együttműködés során kicserélt vagy keletkezett minősített adatok számára.

(2) Jelen Egyezményt kell alkalmazni a minősített adatot érintő minden olyan tevékenység, szerződés vagy megállapodás esetén, amely a Felek, valamint joghatóságuk alá tartozó jogi személyek vagy természetes személyek között jött létre.

(3) Jelen Egyezmény nem érinti a Felek egyéb két-, vagy többoldalú szerződés alapján fennálló, a minősített adatok cseréjével és kölcsönös védelmével kapcsolatos kötelezettségeit.

2. CIKK

FOGALOM-MEGHATÁROZÁSOK

Jelen Egyezmény alkalmazásában:

a) A **minősített adat**: megjelenési formájától, természetétől függetlenül minden olyan adat, amelyet bármelyik Fél országában hatályos jogszabályok és egyéb szabályok rendelkezései szerint védelemben kell részesíteni a minősített adat biztonságának megsértésével szemben, és amelyet ennek megfelelően minősítettek.

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

c) Az **Átadó Fél**: az a Fél, valamint joghatósága alá tartozó azon jogi személy vagy természetes személy, amely az adott országban hatályos jogszabályok és egyéb szabályok rendelkezéseinek megfelelő felhatalmazás alapján minősített adatot ad át.

d) Az **Átvevő Fél**: az a Fél, valamint joghatósága alá tartozó azon jogi személy vagy természetes személy, amely az adott országban hatályos jogszabályok és egyéb szabályok rendelkezéseinek megfelelő meghatalmazás alapján minősített adatot vesz át.

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

f) A **minősítés:** a minősített adaton szereplő jelölés, amely a minősített adat fontosságának mértékére, az adathoz történő hozzáférés korlátozásának fokára és védelmi szintjére utaló minősítési szintet határozza meg.

g) A **szerződő**: olyan jogi személy vagy természetes személy, aki az országában hatályos jogszabályokkal és egyéb szabályokkal összhangban jogképességgel rendelkezik minősített szerződések megkötésére.

h) A **személyi biztonsági tanúsítvány**: nemzetbiztonsági ellenőrzés alapján született pozitív döntés, amely tanúsítja, hogy egy személy az országban hatályos jogszabályok és egyéb szabályok rendelkezései szerint megbízható és megfelel az egyéb biztonsági előírásoknak, ezáltal jogosult hozzáférni minősített adatokhoz.

i) A **telephely biztonsági tanúsítvány**: nemzetbiztonsági ellenőrzés alapján született pozitív döntés, amely tanúsítja, hogy a szerződő az országban hatályos jogszabályok és egyéb szabályok ren-

delkezései szerint a meghatározott minősítési szinten adatokat vehet át, kezelhet, felhasználhat és tárolhat.

j) A **minősített adat biztonságának megsértése**: olyan szándékos vagy véletlen cselekmény vagy mulasztás, amely ellentétes valamelyik Fél országában hatályos jogszabályok és egyéb szabályok rendelkezéseivel, és amelynek eredményeként a minősített adat tényleges vagy feltételezett jogosulatlan hozzáférhetővé tétele következik be, beleértve, de nem kizárólagosan, a minősített adat elvesztését, megsemmisülését, jogosulatlan felhasználását, vagy egyéb módon történő megsértését.

3. CIKK

A HATÁSKÖRREL RENDELKEZŐ BIZTONSÁGI HATÓSÁGOK

(1) A Felek a minősített adatok védelmének felügyeletéért, valamint jelen Egyezmény végrehajtásáért felelős nemzeti biztonsági hatóságai a következők:

Magyarországon:

Nemzeti Biztonsági Felügyelet

A Litván Köztársaságban:

Lietuvos Respublikos paslapčių apsaugos koordinavimo komisija (A Litván Köztársaság Titokvédelmi Koordinációs Bizottsága)

(2) A nemzeti biztonsági hatóságok tájékoztatják egymást hivatalos elérhetőségi adataikról, valamint az ezekkel kapcsolatban bekövetkezett későbbi változásokról.

(3) A nemzeti biztonsági hatóságok tájékoztatják egymást a minősített adatok védelmére kijelölt egyéb, hatáskörrel rendelkező hatóságok hivatalos elérhetőségi adatairól.

4. CIKK

MINŐSÍTÉSI SZINTEK MEGFELELTETÉSE

(1) A Felek rögzítik, hogy az alábbi minősítési szintek megfeleltethetők egymásnak és megegyeznek az érintett országban hatályos jogszabályokban és egyéb szabályokban meghatározott minősítésekkel:

Magyarországon	**A Litván Köztársaságban**	**Angol nyelvű megfelelőjük**
„Szigorúan titkos!”	VISIŠKAI SLAPTAI	TOP SECRET
„Titkos!”	SLAPTAI	SECRET

„Bizalmas!”	KONFIDENCIALIAI	CONFIDENTIAL
„Korlátozott terjesztésű!”	RIBOTO NAUDOJIMO	RESTRICTED

(2) Az Átadó Fél az átadott minősített adat kezelésével kapcsolatban további, a minősítéstől független útmutatást adhat az átadott minősített adat felhasználására vonatkozó részletszabályokról.

5. CIKK

MINŐSÍTETT ADATHOZ VALÓ HOZZÁFÉRÉS

Jelen Egyezmény alapján minősített adathoz kizárólag olyan személyek kaphatnak hozzáférést, akik érvényes személyi biztonsági tanúsítvánnyal rendelkeznek vagy akik a hozzáférésre megfelelő felhatalmazást kaptak az adott országban hatályos jogszabályok és egyéb szabályok rendelkezéseivel összhangban.

6. CIKK

BIZTONSÁGI ALAPELVEK

(1) Az Átvevő Fél:

a) biztosítja, hogy az átvett minősített adaton az Átadó Fél által meghatározott minősítési szinttel egyenértékű minősítés kerüljön feltüntetésre;
b) ugyanolyan szintű védelemben részesíti a minősített adatot, mint amelyet a saját, azonos minősítési szintű minősített adata számára biztosít;
c) biztosítja, hogy a minősített adat minősítését nem szünteti meg, és a minősítési szintjét nem változtatja meg;
d) biztosítja, hogy az Átadó Fél előzetes írásbeli hozzájárulása nélkül az átvett minősített adatot harmadik fél részére nem adja át;
e) a minősített adatot kizárólag az átadás során megjelölt célra használja fel.

(2) Az Átadó Fél haladéktalanul tájékoztatja az Átvevő Felet az adat minősítésében vagy a minősítés időtartamában bekövetkezett változásokról.

7. CIKK

BIZTONSÁGI EGYÜTTMŰKÖDÉS

(1) Az összeegyeztethető szintű biztonsági követelmények fenntartása érdekében a nemzeti biztonsági hatóságok a másik fél megkeresésére tájékoztatják egymást az országukban hatályos, a minősített adat védelmével kapcsolatos jogszabályaikról és egyéb szabályaikról, valamint mindezek gyakorlati alkalmazásáról. A nemzeti biztonsági hatóságok tájékoztatják egymást az országukban hatályos jogszabályaikban és egyéb szabályaikban a minősített adat védelmével kapcsolatban bekövetkezett valamennyi lényeges változásról.

(2) Megkeresés esetén a nemzeti biztonsági hatóságok összhangban az országukban hatályos jogszabályaik és egyéb szabályaik rendelkezéseivel, egyeztetéseket folytatnak le és kölcsönösen segítséget nyújtanak egymásnak a személyi biztonsági tanúsítványokkal és a telephely biztonsági tanúsítványokkal kapcsolatos eljárások során.

(3) A Felek az országukban hatályos jogszabályok és egyéb szabályok rendelkezéseivel összhangban elismerik a másik Fél által kibocsátott biztonsági tanúsítványokat. A jelen Egyezmény 4. cikkében foglaltakat ennek megfelelően kell alkalmazni.

(4) A nemzeti biztonsági hatóságok haladéktalanul értesítik egymást az elismert személyi biztonsági tanúsítványokkal kapcsolatos változásokról, különösen azok visszavonásáról.

(5) A nemzeti biztonsági hatóságok jelen Egyezmény végrehajtása érdekében megállapodásokat köthetnek.

8. CIKK

MINŐSÍTETT SZERZŐDÉSEK

(1) A minősített szerződéseket a Felek országában hatályos jogszabályok és egyéb szabályok rendelkezései alapján kell megkötni és teljesíteni. Az Átadó Fél nemzeti biztonsági hatóságának vagy egyéb, hatáskörrel rendelkező hatóságának kérelmére az Átvevő Fél nemzeti biztonsági hatósága igazolja, hogy a szerződéskötést megelőző tárgyalásokban részt vevő lehetséges szerződő fél vagy a minősített szerződések teljesítésében részt vevő rendelkezik-e megfelelő telephely biztonsági tanúsítvánnyal. Ha a lehetséges szerződő fél nem rendelkezik érvényes telephely biztonsági tanúsítvánnyal, az Átadó Fél nemzeti biztonsági hatósága vagy egyéb, hatáskörrel rendelkező hatósága kezdeményezheti a szerződő biztonsági ellenőrzésének lefolytatását.

(2) A nemzeti biztonsági hatóság vagy egyéb, hatáskörrel rendelkező hatóság kezdeményezheti a minősített adat folyamatos védelmének biztosítása céljából biztonsági ellenőrzés lefolytatását a másik Fél országának területén működő létesítményben.

(3) A minősített szerződések részét képezi a biztonsági melléklet, amely a biztonsági követelményeket és a minősített szerződésben elemeinek minősítési szintjével kapcsolatos rendelkezéseket határozza meg. A biztonsági melléklet másolatát a nemzeti biztonsági hatóságok részére továbbítani kell.

(4) Az Átvevő Fél nemzeti biztonsági hatósága felelős azért, hogy a minősített szerződésekkel kapcsolatban ugyanolyan szabályoknak és követelményeknek megfelelő biztonsági intézkedéseket írjon elő és alkalmazzon, mint amilyet a saját minősített szerződéseinek védelmével kapcsolatban is előír.

9. CIKK

A MINŐSÍTETT ADAT TOVÁBBÍTÁSA

(1) A minősített adat továbbítása az érintett országban hatályos jogszabályokkal és egyéb szabályokkal összhangban, diplomáciai úton vagy katonai futár útján történik.

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

(3) „Titkos!”/ SLAPTAI/ SECRET vagy magasabb minősítési szintű adat továbbítása esetén az Átvevő Fél annak átvételét írásban megerősíti. Az Átadó Fél kérelme alapján az Átvevő Fél megerősíti, hogy a „Korlátozott terjesztésű!”/ NAUDOJIMO/ RESTRICTED vagy „Bizalmas!”/ KONFIDENCIALIAI/ CONFIDENTIAL minősítéssel ellátott minősített adatot átvette.

(4) Minősített adatot tartalmazó nagyméretű küldemény továbbításáról a nemzeti biztonsági hatóságok eseti jelleggel rendelkeznek. A nemzeti biztonsági hatóságok jóváhagyják a szállítás módját, az útvonalat és a biztonsági intézkedéseket.

(5) Az Átadó Fél a minősített adatot olyan formában bocsátja az Átvevő Fél rendelkezésére, amely a szállítás céljának megfelel.

10. CIKK

A MINŐSÍTETT ADAT SOKSZOROSÍTÁSA, FORDÍTÁSA ÉS MEGSEMMISÍTÉSE

(1) Jelen Egyezmény alapján átadott vagy létrehozott minősített adatról készült másolatokon és fordításokon fel kell tüntetni az eredeti minősítést, valamint a hozzárendelt kezelési útmutatást. 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) A minősített adatról másolatot vagy fordítást csak az a természetes személy készíthet, aki felhatalmazást kapott a minősített adat szintjének megfelelő adatokhoz történő hozzáférésre.

(3) Jelen Egyezmény alapján átadott vagy létrehozott minősített adat fordítása során keletkező példányokon fel kell tüntetni a fordítás nyelvén azt, hogy az Átadó Fél minősített adatát tartalmazza.

(4) Jelen Egyezmény alapján átadott vagy létrehozott „Titkos!”/ SLAPTAI/ SECRET vagy magasabb minősítésű adat csak az Átadó Fél előzetes írásbeli engedélyével fordítható vagy sokszorosítható.

(5) A minősített adat megsemmisíthető kivéve, ha az Átadó Fél a kezelési útmutatóban másként határozott. A minősített adatot az érintett országban hatályos jogszabályokkal és egyéb szabályokkal összhangban kell megsemmisíteni. A „Szigorúan titkos!”/ VISIŠKAI SLAPTAI/ TOP SECRET minősítésű adat nem semmisíthető meg, azt az Átadó Félnek kell visszaszolgáltatni, kivéve a jelen cikk (6) bekezdésében meghatározott esetkört.

(6) Olyan válsághelyzet esetén, amikor a minősített adat védelme lehetetlenné válik, a minősített adatot azonnal meg kell semmisíteni. Az Átvevő Fél haladéktalanul értesíti az Átadó Felet a minősített adat megsemmisítéséről.

11. CIKK

LÁTOGATÁSOK

(1) A másik Fél „Bizalmas!”/ KONFIDENCIALIAI/ CONFIDENTIAL vagy magasabb minősítési szintű minősített adatához való hozzáférést igénylő látogatás csak az alábbi hatóságok által kiállított engedéllyel folytatható le:
- Magyarországon a nemzeti biztonsági hatóságként megjelölt hatóság;
- a Litván Köztársaságban a nemzeti biztonsági hatóságként megjelölt hatóság vagy a meglátogatandó igazgatási szerv.

(2) A látogatásra vonatkozó megkeresést legalább húsz nappal a látogatás időpontja előtt kell benyújtani. Sürgős esetben jelen cikk (1) bekezdésében meghatározott hatóságok és szervek 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 ideje és helye, állampolgársága, útlevelének vagy más személyazonosító igazolványának száma;
b) a látogató beosztásának és a látogató által képviselt létesítmény megjelölése;
c) a látogató személyi biztonsági tanúsítványának szintje és érvényességi ideje;
d) a látogatás időpontja és időtartama, visszatérő látogatások esetén az egyes látogatások összesített időtartama;
e) a látogatás célja, valamint a megismerendő legmagasabb minősítési szintű minősített adat minősítési szintjének megjelölése;
f) a meglátogatandó létesítmény neve és címe, valamint a kapcsolattartójának neve, telefonszáma, faxszáma, e-mail címe;
g) dátum, aláírás és a képviselt hatóság hivatalos pecsétjének lenyomata.

(4) Jelen cikk (1) bekezdésében meghatározott hatóságok és szervek közösen meghatározhatják a visszatérő látogatásra jogosult személyek listáját és a visszatérő látogatások további részleteit.

(5) A látogató által megismert minősített adatot úgy kell tekinteni, mint a jelen Egyezmény alapján átvett minősített adatot.

12. CIKK

ELJÁRÁS A MINŐSÍTETT ADAT BIZTONSÁGÁNAK MEGSÉRTÉSE ESETÉN

(1) A nemzeti biztonsági hatóságok késedelem nélkül írásban tájékoztatják egymást a minősített adat biztonságának megsértéséről.

(2) Azon Fél nemzeti biztonsági hatósága, ahol a minősített adat biztonságának megsértésére sor került, késedelem nélkül intézkedik a minősített adat biztonsága megsértésének kivizsgálása

érdekében, és kezdeményezi a körülmények feltárására irányuló eljárások lefolytatását. A másik Fél nemzeti biztonsági hatósága szükség esetén részt vesz a vizsgálatban és az eljárásokban.

(3) Az Átvevő Fél nemzeti biztonsági hatósága minden esetben írásban tájékoztatja az Átadó Fél nemzeti biztonsági hatóságát 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 hatálybalépéséhez szükséges belső jogi feltételek teljesülésére vonatkozó, diplomáciai úton küldött utolsó értesítése kézhezvételének napját követő második hónap első napján lép hatályba.

(2) Jelen Egyezmény a Felek kölcsönös egyetértésével írásban módosítható. A módosítások hatálybalépésével kapcsolatban a jelen cikk (1) bekezdésében foglaltak az irányadók.

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

(4) Az Egyezmény megszűnésétől függetlenül az annak alapján átadott vagy létrehozott minősített adatokat az Egyezményben meghatározott rendelkezések szerint kell védelemben részesíteni, mindaddig, amíg az Átadó Fél írásban felmentést nem ad az Átvevő Fél részére ezen kötelezettség alól.

(5) Felek a jelen Egyezmény értelmezéséből vagy végrehajtásából fakadó vitákat a Felek közötti egyeztetés és tárgyalás útján rendezik.

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

Készült Tallinnban, 2017. szeptember 8-án, két eredeti példányban magyar, litván és angol nyelven, valamennyi szöveg egyaránt hiteles. Eltérő értelmezés esetén az angol nyelvű szöveg az irányadó.”

„AGREEMENT BETWEEN

THE GOVERNMENT OF HUNGARY

AND

THE GOVERNMENT OF THE REPUBLIC OF LITHUANIA

ON THE EXCHANGE AND MUTUAL PROTECTION

OF CLASSIFIED INFORMATION

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

Recognising the important role of the mutual political, economic and military cooperation,

Realising that good co-operation may require exchange or generation of classified information,

Recognising that they ensure equivalent protection for the classified information,

Wishing to ensure the protection of classified information exchanged or generated in the course of co-operation,

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

ARTICLE 1
OBJECTIVE AND 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.

2. This Agreement shall be applicable to any activities, contracts or agreements involving classified information that are conducted or concluded between the Parties including any entity under its jurisdiction.

3. This Agreement shall not affect the obligations of the Parties under any other bilateral or multilateral treaty concerning 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 laws and regulations in force in the state of either Party, requires protection against breach of security and has been duly designated.

b) **"classified contract"** means a contract or subcontract that involves or requires access to classified information.

c) **"Originating Party"** means the Party including any entity under its jurisdiction, which, having the capacity to do so under the laws and regulations in force in their states, releases classified information.

d) **"Recipient Party"** means the Party including any entity under its jurisdiction, which, having the capacity to do so under the laws and regulations in force in their states, receives classified information.

e) **"third party"** means any state including any entity under its jurisdiction or international organisation not being a party to this Agreement.

f) **"classification"** means a mark assigned to classified information, which indicates the classification level and characterizes the importance of classified information, level of restriction of access to it and level of protection.

g) "**contractor**" means any entity possessing the legal capacity to conclude classified contracts in accordance with the laws and regulations in force in its state.

h) "**Personnel Security Clearance Certificate**" means a positive determination stemming from a national vetting procedure that shall ascertain loyalty and trustworthiness as well as other security

aspects of an individual in accordance with the laws and regulations in force in its state and confirms that an individual is eligible to have access to classified information.

i) "**Facility Security Clearance Certificate**" means a positive determination stemming from a national vetting procedure that a contractor in accordance with the laws and regulations in force in its state is authorized to receive, handle, process and store classified information up to a certain classification level.

j) „**breach of security**" means a deliberate or accidental act or an omission contrary to the laws and regulations in force in the state of either Party, the result of which may lead to an actual or presumed unauthorised disclosure of classified information, including but not limited to its loss, destruction, damage, misappropriation or misuse.

ARTICLE 3
COMPETENT SECURITY AUTHORITIES

1. The national security authorities of the Parties responsible for the control of the protection of classified information as well as the implementation of this Agreement are:

In Hungary:
Nemzeti Biztonsági Felügyelet (National Security Authority);

In the Republic of Lithuania:
Lietuvos Respublikos paslapčių apsaugos koordinavimo komisija (Commission for secrets protection coordination of the Republic of Lithuania).

2. The national security authorities shall provide each other with official contact details and shall inform each other of any subsequent changes thereof.

3. The national security authorities shall provide each other with official contact details of other competent authorities responsible for the designated fields of protection of classified information.

ARTICLE 4
CLASSIFICATIONS

1. The Parties agree that the following classifications are equivalent and correspond to the classifications specified in the laws and regulations in force in the respective state:

In Hungary	In the Republic of Lithuania	Equivalent in the English language
„Szigorúan titkos!”	VISIŠKAI SLAPTAI	TOP SECRET
„Titkos!”	SLAPTAI	SECRET
„Bizalmas!”	KONFIDENCIALIAI	CONFIDENTIAL
“Korlátozott terjesztésű!”	RIBOTO NAUDOJIMO	RESTRICTED

2. The Originating Party apart from the classification may provide any further handling instructions which detail the use of the transferred classified information.

ARTICLE 5
ACCESS TO CLASSIFIED INFORMATION

Access to classified information under this Agreement shall be limited only to individuals, who have been issued an appropriate Personnel Security Clearance Certificate or who are duly authorized in accordance with the laws and regulations in force in their state.

ARTICLE 6
SECURITY PRINCIPLES

1. The Recipient Party shall:

a) ensure that the received classified information is marked with an equivalent classification corre-

sponding to the classification specified by the Originating Party;
b) afford the same degree of protection to classified information as afforded to its own classified information of an equivalent classification level;
c) ensure that classified information is not declassified nor its classification level is changed;
d) ensure that classified information is not released to a third party without the prior written consent of the Originating Party;
e) use classified information only for the purpose it has been released for.

2. The Originating Party shall inform the Recipient Party without undue delay of any subsequent changes in the classification level or duration of classification.

ARTICLE 7
SECURITY CO-OPERATION

1. In order to maintain comparable standards of security, the national security authorities shall, on request, inform each other of the laws and regulations in force in their states concerning protection of classified information and the practices stemming from their implementation. The national security authorities shall inform each other of any substantive changes of the laws and regulations in force in their states concerning the protection of classified information.

2. On request, the national security authorities shall, in accordance with the laws and regulations in force in their states hold consultations and assist each other during the personnel security clearance procedures and facility security clearance procedures.

3. The Party shall recognise the Security Clearance Certificates issued by the other Party in accordance with the laws and regulations in force in their states. Article 4 of this Agreement shall apply accordingly.

4. The national security authorities shall promptly notify each other about changes in the recognised Security Clearance Certificates, especially in case of their withdrawal.

5. The national security authorities may conclude implementing arrangements in relation with this Agreement.

ARTICLE 8
CLASSIFIED CONTRACTS

1. Classified contracts shall be concluded and implemented in accordance with the laws and regulations in force in the state of each Party. On request of the national security authority or competent security authority of the Originating Party, the national security authority of the Recipient Party shall confirm if the proposed contractor participating in the pre-contractual negotiations or in the implementation of the classified contract has an appropriate Facility Security Clearance Certificate. If the proposed contractor does not hold an appropriate Facility Security Clearance Certificate, the national security authority or competent security authority of the Originating Party may request its counterpart for that contractor to be security cleared.

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

3. Classified contracts shall contain security annex on the security requirements and on the classification level of each element of the classified contract. A copy of the security annex shall be forwarded to the national security authorities.

4. The national security authority of the Recipient Party shall assume the responsibility for prescribing and administering security measures for the classified contract under the same standards and requirements that govern the protection of its own classified contracts.

ARTICLE 9
TRANSFER AND TRANSMISSION OF CLASSIFIED INFORMATION

1. Classified information shall be transfered in accordance with laws and regulations in force in the respective state through diplomatic channels or military couriers.

2. The Parties may transmit classified information by electronic means in accordance with the security procedures approved by the national security authorities or competent security authorities.

3. If transferred classified information is marked „Titkos!”/ SLAPTAI/ SECRET or above the Recipient Party shall confirm it in writing. Upon request made by the Originating Party, the Recipient Party shall confirm that the classified information marked “Korlátozott terjesztésű!”/ NAUDOJIMO/ RESTRICTED or „Bizalmas!”/ KONFIDENCIALIAI/ CONFIDENTIAL was received.

4. In case of transferring a large consignment containing classified information such transfer must be organised between the national security authorities on a case by case basis. The national security authorities shall confirm the means of transportation, the route and the security measures.

5. The Originating Party shall provide classified information to the Recipient Party in a form which will serve for the purposes of the transfer.

ARTICLE 10
REPRODUCTION, TRANSLATION AND DESTRUCTION OF CLASSIFIED INFORMATION

1. Reproductions and translations of classified information exchanged or generated under this Agreement shall bear original classifications and additional handling instructions thereon and shall be protected as the originals. Number of reproductions shall be limited to that required for official purposes.

2. All translations and reproductions of classified information shall be made by individuals authorised to have access to classified information of the respective classification level.

3. Translations of classified information exchanged or generated under this Agreement shall bear a note in the language of translation indicating that they contain classified information of the Originating Party.

4. Classified information exchanged or generated under this Agreement marked „Titkos!”/ SLAPTAI/ SECRET or above shall be translated or reproduced only upon the prior written consent of the Originating Party.

5. Classified information may be destroyed unless the Originating Party indicates otherwise in handling instructions. The classified information shall be destroyed in accordance with laws and regulations in force in respective state. Classified information marked „Szigorúan titkos!”/ VISIŠKAI SLAPTAI/ TOP SECRET shall not be destroyed but shall be returned to the Originating Party except in case defined in paragraph 6 of this Article.

6. In case of crisis situation, which makes it impossible to protect the classified information it shall be destroyed immediately. The Recipient Party shall notify the Originating Party about the destruction of the classified information as soon as possible.

ARTICLE 11
VISITS

1. Visits requiring access to classified information marked „Bizalmas!”/ KONFIDENCIALIAI/ CONFIDENTIAL or above of the other Party shall have a permission issued:
- for Hungary – by the national security authority;
- for the Republic of Lithuania – by the national security authority or administrative entity to be visited.

2. Requests for visit shall be submitted at least twenty 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 authorities and entities defined in paragraph 1 of this article.

3. Requests for visit shall contain:
a) visitor’s name, date and place of birth, nationality and passport/ID card number;
b) position of the visitor and specification of the legal entity represented;
c) visitor’s Personnel Security Clearance Certificate 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) name and address of the facility to be visited, as well as the name, phone/fax number, e-mail ad-

dress of its point of contact;
g) date, signature and stamping of the official seal of the legal entity represented.

4. The authorities and entities defined in paragraph 1 of this article may agree on a list of visitors entitled to recurring visits and shall agree on the further details of the recurring visits.

5. Classified information acquired by a visitor shall be considered as classified information received under this Agreement.

ARTICLE 12
BREACH OF SECURITY

1. The national security authorities shall without undue delay inform each other in writing of a breach of security.

2. The national security authority of the Party where the breach of security occurred, shall inspect the incident and initiate other appropriate proceedings to determine the circumstances of the breach without delay. The other national security authority shall, if required, co-operate in the investigation and the proceedings.

3. In any case, the national security authority of the Recipient Party shall inform the national security authority of the Originating Party in writing about the circumstances of the breach of security, the extent of the damage, the measures adopted for its mitigation and the outcome of the investigation.

ARTICLE 13
EXPENSES

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

ARTICLE 14
FINAL PROVISIONS

1. This Agreement is concluded for an indefinite period of time. This Agreement shall enter into force on the first day of the second month following the date of receipt of the last of notifications between the Parties, through diplomatic channels, stating that the national legal requirements for this Agreement to enter into force have been fulfilled.

2. This Agreement may be amended on the basis of the mutual agreement of the Parties in writing. Such amendments shall enter into force in accordance with Paragraph 1 of this Article.

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

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

5. Any dispute regarding the interpretation or implementation of this Agreement shall be resolved by consultations and negotiations between the Parties.

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

Done in Tallinn on 8th of September 2017 in two originals, in Hungarian, Lithuanian and English languages, each text being equally authentic. In case of different interpretation the English text shall prevail."

4. §

(1) Ez a törvény – a (2) bekezdésben meghatározott kivétellel – a kihirdetését követő napon lép hatályba.
(2) A 2. § és 3. § az Egyezmény 14. Cikk (1) bekezdésében 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.

5. §

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

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

ÁLTALÁNOS INDOKOLÁS

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

A minősített adatok cseréjére vonatkozó biztonsági együttműködés érdekében – a katonai megállapodások kivételével – hazánk jogszabályi felhatalmazás hiányában korábban csak két állammal, az Olasz Köztársasággal és a Németországi Szövetségi Köztársasággal kötött általános titokvédelmi egyezményt[1] amelyek alkalmazását a 2010. március 31-ig hatályos, az államtitokról és szolgálati titokról szóló 1995. évi LXV. törvény nem tette lehetővé.
A Mavtv. 2010. április 1-jei hatálybalépésével azonban megteremtette a kétoldalú titokvédelmi megállapodások megkötéséhez és alkalmazásához szükséges jogi alapokat, és így megkezdődhetett hazánk e téren tapasztalható elmaradásának felszámolása[2]. Ennek megfelelően hazánk a 46/2011. (VI. 21.) ME határozat értelmében először a Szlovák Köztársasággal, a Lengyel Köztársasággal és a Cseh Köztársasággal kezdte meg a tárgyalásokat, amelyek eredményeképpen 2012. május 3-án aláírásra került Budapesten a Szlovák Köztársaság és Magyarország, 2012. június 13-án a Cseh Köztársaság és Magyarország, 2014. január 29-én a Lengyel Köztársaság és Magyarország közötti megállapodás. Továbbá az 58/2012. (V. 16.) ME határozat alapján 2012. augusztus 29-én a Lett Köztársaság és Magyarország, 2012. december 11-én a Francia Köztársaság és Magyarország, 2013. március 22-én az Osztrák Köztársaság és Magyarország között hasonló megállapodást, valamint az

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.

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 hat megállapodás aláírására került sor; 2016. január 22-én a Szlovén Köztársasággal, 2016. június 10-én a Horvát Köztársasággal, 2016. június 15-én Spanyolországgal, 2016. szeptember 7-én az Oroszországi Föderációval, 2016. október 6-án Montenegróval és 2016. december 7-én az Észt Köztársasággal. 2017. július 5-én került aláírásra a minősített adatvédelmi megállapodás a Bolgár Köztársasággal, 2017. október 25-én pedig a Svéd Királysággal, valamint ugyanazon a napon a Finn Köztársasággal.

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 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.