MAGYARORSZÁG KORMÁNYA

T/17303. számú

törvényjavaslat

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

Előadó: **Dr. Pintér Sándor**
belügyminiszter

Budapest, 2017. augusztus

2017. évi … törvény

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

1. §

Az Országgyűlés e törvénnyel felhatalmazást ad a Magyarország Kormánya és az Olasz 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 AZ OLASZ KÖZTÁRSASÁG KORMÁNYA KÖZÖTT
A MINŐSÍTETT ADATOK CSERÉJÉRŐL ÉS KÖLCSÖNÖS VÉDELMÉRŐL

Magyarország Kormánya és az Olasz Köztársaság Kormánya, a továbbiakban együtt: „Felek”,

Elismerve a Felek közötti kölcsönös együttműködés jelentőségét,

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

Elismerve az azonos szintű védelem biztosításának igényét a minősített adatok számára,

Új egyezménnyel kívánva kiváltani a Magyar Köztársaság Kormánya és az Olasz Köztársaság Kormánya között a minősített információk kölcsönös védelméről szóló, 2003. március 20-án aláírt Biztonsági Megállapodást,

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

1. CIKK
AZ EGYEZMÉNY CÉLJA ÉS ALKALMAZÁSI TERÜLETE

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

2. Jelen Egyezmény nem érinti a Felek egyéb két-, vagy többoldalú szerződés, különösen NATO szerződés alapján fennálló vagy Európai Uniós tagságból eredő kötelezettségeit, ideértve mindazon megállapodásokat is, amelyek minősített adatok cseréjét és kölcsönös védelmét szabályozzák.

2. CIKK
FOGALOMMEGHATÁROZÁSOK

Jelen Egyezmény alkalmazásában:

a) A „**Minősített Adat**” megjelenési formájától vagy természetétől függetlenül, minden olyan adat, amelyet bármelyik Fél nemzeti jogszabályai vagy egyéb szabályai szerint védelemben kell részesíteni a minősített adat biztonságának megsértésével szemben, s amelyet ennek megfelelően minősítettek;

b) A „**Minősített adat biztonságának megsértése**” olyan, a jelen Egyezménnyel és a Felek saját nemzeti jogszabályaival vagy egyéb szabályaival ellentétes tevékenységet vagy mulasztást jelent, melynek következtében a minősített adat jogosulatlan nyilvánosságra hozatala, elvesztése, megsemmisülése, jogosulatlan felhasználása, megszerzése vagy egyéb módon történő megsértése következhet be;

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

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

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

f) A „**Szükséges Ismeret**” azt a követelményt jelenti, amely alapján egy meghatározott minősített adathoz való hozzáférés csak annak a személynek biztosítható, akinek a hozzáférés hivatali kötelessége vagy meghatározott feladata ellátásához igazoltan szükséges;

g) A „**Személyi Biztonsági Tanúsítvány**” a Nemzeti Biztonsági Felügyelet azon döntése, amely szerint a természetes személy a nemzeti jogszabályok és egyéb szabályok rendelkezéseinek tiszteletben tartásával hozzáférhet „Bizalmas!”/ RISERVATISSIMO/ CONFIDENTIAL vagy magasabb szintű minősített adatokhoz;

h) A „**Minősített szerződés**” olyan szerződést jelent, amely minősített adatot tartalmaz vagy amely alapján minősített adathoz történő hozzáférés szükséges;

i) A „**Szerződő**” olyan természetes személy vagy jogi személy, amely a nemzeti jogszabályok vagy egyéb szabályok rendelkezéseivel összhangban jogképességgel rendelkezik minősített szerződések megkötésére;

j) A „**Telephely Biztonsági Tanúsítvány**” a Nemzeti Biztonsági Felügyelet azon döntése, amely szerint a jogképességgel rendelkező jogi személy vagy természetes személy rendelkezik azon fizikai és szervezeti képességekkel, amely alkalmassá teszik a „Bizalmas!”/ RISERVATISSIMO/ CONFIDENTIAL vagy magasabb szintű minősített adatok kezelésére és tárolására a nemzeti jogszabályok és egyéb szabályok rendelkezéseinek megfelelően;

k) A „**Nemzeti Biztonsági Felügyelet**” az a nemzeti hatóság, amely a minősített adatok védelme vonatkozásában felelős a nemzeti jogszabályok és egyéb szabályok rendelkezéseinek pontos betartásáért, valamint jelen Egyezmény alkalmazásáért és felügyeletéért.

3. CIKK
NEMZETI BIZTONSÁGI FELÜGYELETEK

1. A Felek Nemzeti Biztonsági Felügyeletei a következők:

Magyarországon:
Nemzeti Biztonsági Felügyelet

Az Olasz Köztársaságban:
Információbiztonsági Osztály-Nemzeti Biztonsági Testület (Dipartimento delle Informazioni per la Sicurezza – Organo Nazionale di Sicurezza)

2. A Nemzeti Biztonsági Felügyeletek kötelesek tájékoztatni egymást hivatalos elérhetőségi adataikról, valamint az ezzel kapcsolatos változásokról.

4. CIKK
MINŐSÍTÉSI SZINTEK MEGFELELTETÉSE

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

Magyarországon	**Az Olasz Köztársaságban**	**Angol nyelvű megfelelőjük**
„Szigorúan titkos!”	SEGRETISSIMO	TOP SECRET
„Titkos!”	SEGRETO	SECRET
„Bizalmas!”	RISERVATISSIMO	CONFIDENTIAL
„Korlátozott terjesztésű!”	RISERVATO	RESTRICTED

5. CIKK
MINŐSÍTETT ADATHOZ VALÓ HOZZÁFÉRÉS

Minősített adathoz jelen Egyezmény alapján kizárólag olyan természetes személyek jogosultak hozzáférni, akik a Szükséges Ismeret elvének megfelelnek és az érintett Fél nemzeti jogszabályaival és egyéb szabályaival összhangban erre megfelelő felhatalmazást kaptak.

6. CIKK
BIZTONSÁGI ALAPELVEK

1. Az Átadó Fél:

a) köteles biztosítani, hogy a minősített adaton a nemzeti jogszabályai és egyéb szabályai szerinti megfelelő minősítési szint feltüntetésre kerüljön;

b) köteles tájékoztatni az Átvevő Felet a minősített adat felhasználásának esetleges feltételhez kötéséről;

c) haladéktalanul köteles írásban tájékoztatni az Átvevő Felet az adat minősítési szintjében bekövetkezett változásokról.

2. Az Átvevő Fél:

a) köteles biztosítani, hogy a minősített adaton feltüntetésre kerüljön jelen Egyezmény 4. Cikke alapján meghatározott egyenértékű minősítési szint;

b) ugyanolyan szintű védelemben köteles részesíteni a másik Féltől kapott minősített adatot, mint amelyet a saját, azonos minősítési szintű minősített adata számára biztosít;

c) köteles biztosítani, hogy az Átadó Fél előzetes írásbeli hozzájárulása nélkül a minősített adat minősítését nem szüntetik meg, illetve minősítési szintjét nem változtatják meg;

d) köteles biztosítani, hogy az Átadó Fél előzetes írásbeli hozzájárulása nélkül az átvett minősített adatot Harmadik Fél részére nem adja át;

e) a minősített adatot kizárólag az átadás során megjelölt célra használhatja fel, betartva az Átadó Fél által meghatározott feltételeket.

7. CIKK
BIZTONSÁGI EGYÜTTMŰKÖDÉS

1. A hasonló szintű biztonsági követelmények fenntartása érdekében a Nemzeti Biztonsági Felügyeletek megkeresésre kötelesek egymást tájékoztatni a minősített adat védelmével kapcsolatos nemzeti jogszabályokról és egyéb szabályokról, valamint mindezek gyakorlati alkalmazásáról.

2. Megkeresés esetén a Nemzeti Biztonsági Felügyeletek, kötelesek egymással együttműködni és egymásnak segítséget nyújtani a személyi biztonsági tanúsítványok kiállításával kapcsolatos biztonsági ellenőrzések során.

3. A Felek kötelesek nemzeti jogszabályaik és egyéb szabályaik rendelkezéseivel összhangban elismerni a másik Fél által, jelen Egyezmény 4. Cikkében foglaltaknak megfelelően kibocsátott személyi biztonsági tanúsítványokat és telephely biztonsági tanúsítványokat.

4. A Nemzeti Biztonsági Felügyeletek vagy más, hatáskörrel rendelkező biztonsági szervezetek kötelesek nemzeti jogszabályaik és egyéb szabályaik rendelkezéseivel összhangban, haladéktalanul

értesíteni egymást az elismert személyi biztonsági tanúsítványokkal és a telephely biztonsági tanúsítványokkal kapcsolatos változásokról, különösen azok visszavonásáról.

5. Jelen Egyezmény során megvalósuló együttműködés angol nyelven történik.

8. CIKK
MINŐSÍTETT SZERZŐDÉSEK

1. A minősített szerződéseket a Felek saját nemzeti jogszabályai és egyéb szabályai alapján kell megkötni és teljesíteni. A Nemzeti Biztonsági Felügyeletek megkeresésre kötelesek megerősíteni, hogy az ajánlattevők és a szerződéskötést megelőző tárgyalásokban vagy a „Bizalmas!”/ RISERVATISSIMO/ CONFIDENTIAL vagy magasabb minősítési szintre minősített szerződések teljesítésében részt vevő természetes személyek rendelkeznek megfelelő személyi biztonsági tanúsítvánnyal vagy telephely biztonsági tanúsítvánnyal.

2. A Nemzeti Biztonsági Felügyelet információt kérhet a másik Fél Nemzeti Biztonsági Felügyeletétől a másik Fél területén lévő létesítményre vonatkozó biztonsági helyzettel kapcsolatban a minősített adat folyamatos védelmének biztosítása céljából.

3. A „Bizalmas!”/ RISERVATISSIMO/ CONFIDENTAL vagy magasabb minősítési szintre minősített szerződések lényeges részét képezi a projekt biztonsági utasítás, amely a biztonsági követelményeket és a minősített szerződés egyes elemeinek minősítésével kapcsolatos rendelkezéseket határozza meg. A projekt biztonsági utasítás másolatát azon Fél Nemzeti Biztonsági Felügyelete részére kell továbbítani, amelynek joghatósága alatt a minősített szerződés végrehajtása történik.

4. A „Korlátozott terjesztésű!”/ RISERVATO/ RESTRICTED minősítésű minősített szerződés biztonsági záradékot tartalmaz, amely a minősített adat védelmét biztosító minimum biztonsági intézkedéseket határozza meg.

9. CIKK
A MINŐSÍTETT ADAT TOVÁBBÍTÁSA

1. A minősített adat továbbítása az Átadó Fél nemzeti jogszabályaiban és egyéb szabályaiban meghatározott szabályok szerint, diplomáciai úton, vagy a Nemzeti Biztonsági Felügyeletek által írásban meghatározott egyéb módon történik.

2. A Felek, a Nemzeti Biztonsági Felügyeletek által írásban jóváhagyott eljárási rend szerint, elektronikus úton is továbbíthatnak minősített adatot.

10. CIKK
A MINŐSÍTETT ADAT SOKSZOROSÍTÁSA, FORDÍTÁSA ÉS MEGSEMMISÍTÉSE

1. Jelen Egyezmény alapján átadott minősített adatról készült másolatokon és fordításokon fel kell tüntetni a megfelelő minősítési jelölést és az így készült adatot ugyanolyan védelemben kell részesíteni, mint az eredeti minősített adatot. A sokszorosított példányok számát a hivatalos célból szükséges mértékre kell korlátozni.

2. Jelen Egyezmény alapján átadott minősített adat fordítása során keletkező példányokon a fordítás nyelvén fel kell tüntetni, hogy az az Átadó Fél minősített adatát tartalmazza.

3. Jelen Egyezmény alapján átadott, „Szigorúan titkos!”/ SEGRETISSIMO/ TOP SECRET minősítésű adat fordítása vagy sokszorosítása kizárólag az Átadó Fél előzetes írásbeli engedélyével lehetséges.

4. Jelen Egyezmény alapján átadott, „Szigorúan titkos!”/ SEGRETISSIMO/ TOP SECRET minősítésű adat nem semmisíthető meg, az ezen minősítési szintű adatokat az Átadó Félnek kell visszaszolgáltatni.

5. Olyan válsághelyzet esetén, amely lehetetlenné teszi a minősített adat védelmét, vagy az Átadó Félnek való visszajuttatását, a minősített adatot haladéktalanul meg kell semmisíteni. Az Átvevő Fél Nemzeti Biztonsági Felügyelete köteles az Átadó Fél Nemzeti Biztonsági Felügyeletét írásban értesíteni a minősített adatok megsemmisítéséről.

11. CIKK
LÁTOGATÁSOK

1. Minősített adathoz való hozzáférést igénylő látogatásra az érintett Nemzeti Biztonsági Felügyelet előzetes írásbeli jóváhagyása alapján kerülhet sor.

2. A látogató Fél Nemzeti Biztonsági Felügyelete köteles a fogadó Fél Nemzeti Biztonsági Felügyeletét látogatásra vonatkozó megkeresésében legalább húsz nappal a látogatás időpontja előtt tájékoztatni a tervezett látogatásról. Sürgős esetben, a Nemzeti Biztonsági Felügyeletek előzetes egyeztetését követően a látogatásra vonatkozó megkeresés a látogatás kezdetéhez közelebbi időpontban is benyújtható.

3. A látogatásra vonatkozó megkeresésnek az alábbiakat kell tartalmaznia:

a) a látogató neve, születési helye és ideje, állampolgársága, útlevelének vagy más személyazonosító igazolványának száma;

b) a látogató beosztásának és a látogató által képviselt jogi személynek a 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 Nemzeti Biztonsági Felügyelet hivatalos pecsétjének lenyomata.

4. A Nemzeti Biztonsági Felügyeletek közösen meghatározhatják a visszatérő látogatásra jogosult személyek listáját. Azon projektek vagy szerződések esetén, amelyben szükséges a látogatás megismétlése a Felek Nemzeti Biztonsági Felügyeletei kötelesek egymást tájékoztatni a felhatalmazott személyek listájának megküldésével nemzeti jogszabályaik és egyéb szabályaik rendelkezéseivel összhangban. A lista érvényessége nem lehet hosszabb, mint tizenkét hónap. Amennyiben a lista elfogadásra kerül, a látogatások a nemzeti jogszabályok és egyéb szabályok rendelkezéseivel összhangban közvetlenül lefolytathatók.

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 Felügyeletek késedelem nélkül írásban tájékoztatják egymást a minősített adat biztonságának megsértéséről vagy ennek alapos gyanújáról.

2. Azon Fél Nemzeti Biztonsági Felügyelete, ahol a minősített adat biztonságának megsértésére sor került, késedelem nélkül intézkedik a minősített adat megsértésének kivizsgálása érdekében. A másik Fél Nemzeti Biztonsági Felügyelete szükség esetén részt vesz a vizsgálatban.

3. Az Átvevő Fél Nemzeti Biztonsági Felügyelete minden esetben írásban tájékoztatja az Átadó Fél Nemzeti Biztonsági Felügyeletét a minősített adat biztonsága megsértésének körülményeiről, a kár mértékéről, a kár enyhítése érdekében megtett intézkedésekről, valamint a vizsgálat eredményéről.

4. Ha a minősített adat biztonságának megsértése harmadik Félnél következik be, az a Nemzeti Biztonsági Felügyelet, amely a minősített adatot a harmadik Félnek átadta köteles megtenni minden lehetséges intézkedést jelen Cikkben meghatározott előírások megvalósulásának biztosítása érdekében.

13. CIKK
KÖLTSÉGEK VISELÉSE

Jelen Egyezmény végrehajtása nem jár költségekkel. Az esetlegesen mégis felmerülő költségeket a Felek maguk viselik.

14. CIKK
ZÁRÓ RENDELKEZÉSEK

1. Jelen Egyezmény határozatlan időre jön létre. Jelen Egyezmény a Felek az Egyezmény hatálybalépéshez szükséges belső feltételek teljesítésére vonatkozó, diplomáciai úton küldött utolsó értesítése kézhezvételének napját követő második hónap első napján lép hatályba.

2. Jelen Egyezmény a Felek kölcsönös egyetértésével írásban módosítható. A módosítások hatályba lépésével kapcsolatban a jelen Cikk 1. pontjában foglaltak az irányadók.

3. Bármelyik Fél jogosult jelen Egyezményt bármikor írásban felmondani. Felmondás esetén az Egyezmény a felmondásról szóló írásbeli értesítés másik Fél általi kézhezvételétől számított 6 hónap elteltével hatályát veszti.

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

5. Felek a jelen Egyezmény értelmezéséből vagy végrehajtásából fakadó vitákat tárgyalás és egyeztetés útján, külső igazságszolgáltatási fórum igénybe vétele nélkül rendezik.

6. Jelen Egyezmény hatályba lépésével a Magyar Köztársaság Kormánya és az Olasz Köztársaság Kormánya között a minősített információk kölcsönös védelméről szóló 2003. március 20-án aláírt Biztonsági Megállapodás hatályát veszti.

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

Készült Budapesten, 2015. november 26-án, két eredeti példányban, magyar, olasz és angol nyelven, valamennyi szöveg egyaránt hiteles. Eltérés esetén az angol nyelvű szöveg az irányadó.

Magyarország Kormánya részéről	**Az Olasz Köztársaság Kormánya részéről”**

“AGREEMENT
BETWEEN THE GOVERNMENT OF HUNGARY AND THE GOVERNMENT OF THE ITALIAN REPUBLIC ON THE EXCHANGE AND MUTUAL PROTECTION OF CLASSIFIED INFORMATION

The Government of Hungary and the Government of the Italian Republic, hereinafter referred to as the “Parties”,

Recognising the importance of mutual cooperation between the Parties,

Realising that good cooperation may require exchange of Classified Information between the Parties,

Recognising the interest that the Parties ensure equivalent protection for the Classified Information,

Wishing to replace the Agreement between the Government of the Italian Republic and the Government of the Republic of Hungary on the mutual protection of Classified Information signed on 20th March 2003 with a new Agreement,

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

ARTICLE 1
OBJECTIVE AND APPLICABILITY OF THE AGREEMENT

1. The objective of this Agreement is to ensure the protection of Classified Information exchanged or generated in the framework of the cooperation between the Parties or between the legal entities or individuals under their jurisdiction.

2. This Agreement shall not affect the obligations of the Parties under any other bilateral or multilateral treaty, in particular NATO treaty, or obligations stemming from EU membership, including any agreements governing exchange and mutual protection of Classified Information.

ARTICLE 2
DEFINITIONS

For the purpose of this Agreement:

a) **“Classified Information”** means any information that, regardless of its form or nature, under the national laws and regulations of either Party, requires protection against breach of security and has been duly designated;

b) **“Breach of Security**” means an act or an omission which is contrary to this Agreement or to the national laws and regulations of the respective Parties, the result of which may lead to unauthorised disclosure, loss, destruction, access, misappropriation or any other type of compromise of Classified Information;

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

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

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

f) **"Need-to-know**" means the principle, according to which access to specific Classified Information may only be granted to a person who has a verified need to access this Classified Information in connection with his/her official duties or for the performance of a specific task;

g) **"Personnel Security Clearance Certificate**" means the determination by the National Security Authority confirming that an individual is eligible to have access to information classified "Bizalmas!"/ RISERVATISSIMO/ CONFIDENTIAL or above, in accordance with the national laws and regulations;

h) **"Classified Contract"** means a contract that involves or requires access to Classified Information;

i) **"Contractor**" means an individual or a legal entity possessing the legal capacity to conclude Classified Contracts in accordance with the national laws and regulations;

j) **"Facility Security Clearance Certificate**" means the determination by the National Security Authority confirming that a legal entity or an individual possessing the legal capacity, has the physical and organizational capability to handle and store information classified "Bizalmas!"/ RISERVATISSIMO/ CONFIDENTIAL or above in accordance with the national laws and regulations;

k) **"National Security Authority**" means the national authority competent to ensure the correct implementation of the national laws and regulations in the field of protection of Classified Information and which is responsible for the application and supervision of this Agreement.

ARTICLE 3
NATIONAL SECURITY AUTHORITIES

1. The National Security Authorities of the Parties are:

In Hungary:
Nemzeti Biztonsági Felügyelet
(National Security Authority)

In the Italian Republic:
Dipartimento delle Informazioni per la Sicurezza – Organo Nazionale di Sicurezza
(Department of Information for Security –National Security Body)

2. The National Security Authorities shall provide each other with official contact details and shall inform each other of any subsequent changes thereof.

ARTICLE 4
SECURITY CLASSIFICATION LEVELS AND MARKINGS

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

In Hungary	In the Italian Republic	Equivalent in English language
„Szigorúan titkos!”	SEGRETISSIMO	TOP SECRET
„Titkos!”	SEGRETO	SECRET
„Bizalmas!”	RISERVATISSIMO	CONFIDENTIAL
„Korlátozott terjesztésű!”	RISERVATO	RESTRICTED

ARTICLE 5
ACCESS TO CLASSIFIED INFORMATION

Access to Classified Information under this Agreement shall be limited only to individuals upon the Need-to-know principle and who are duly authorized in accordance with the national laws and regulations of the respective Party.

ARTICLE 6
SECURITY PRINCIPLES

1. The Originating Party shall:

a) ensure that Classified Information is marked with appropriate security classification markings in accordance with its national laws and regulations;

b) inform the Recipient Party of any use conditions of Classified Information;

c) inform the Recipient Party in writing without undue delay of any subsequent changes in the security classification level.

2. The Recipient Party shall:

a) ensure that Classified Information is marked with equivalent security classification marking in accordance with Article 4 of this Agreement;

b) afford Classified Information received from the other Party a level of security protection that is

afforded to its own Classified Information of an equivalent classification level;

c) ensure that Classified Information is not declassified nor its security classification level changed without the prior written consent of the Originating Party;

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 and in accordance with release conditions of the Originating Party.

ARTICLE 7
SECURITY COOPERATION

1. In order to maintain comparable standards of security, the National Security Authorities shall, on request, inform each other of their national laws and regulations concerning protection of Classified Information and the practices deriving from their implementation.

2. On request, the National Security Authorities, shall cooperate and give mutual assistance during the vetting procedures for the release of Personnel Security Clearances.

3. The Parties shall, in accordance with their national laws and regulations, recognise the personnel security clearance certificates and facility security clearance certificates issued by the other Party accordingly to Article 4 of this Agreement.

4. The National Security Authorities or other competent security organizations in accordance with national laws and regulations shall promptly notify each other about changes in the recognised personnel security clearance certificates and facility security clearance certificates, especially in case of their withdrawal.

5. The cooperation under this Agreement shall be effected in the English language.

ARTICLE 8
CLASSIFIED CONTRACTS

1. Classified contracts shall be concluded and implemented in accordance with the national laws and regulations of each Party. On request, the National Security Authorities shall confirm that proposed contractors as well as individuals participating in pre-contractual negotiations or in the implementation of contracts classified “Bizalmas!”/ RISERVATISSIMO/ CONFIDENTIAL and above have appropriate personnel Security Clearance Certificate or Facility Security Clearance Certificate.

2. The National Security Authority may request its counterpart information regarding security situation concerning a facility located in the territory of the other Party to ensure continuing protection of Classified Information.

3. Contracts classified “Bizalmas!”/ RISERVATISSIMO/ CONFIDENTIAL and above shall contain, as integral part of the contract, project security instructions on the security requirements

and on the security classification level of each element of the Classified Contract. A copy of the project security instructions shall be forwarded to the National Security Authority of the Party under whose jurisdiction the Classified Contract is to be implemented.

4. Contracts classified "Korlátozott terjesztésű!"/ RISERVATO/ RESTRICTED shall contain an appropriate security clause identifying the minimum security measures to be applied for the protection of Classified Information.

ARTICLE 9
TRANSMISSION OF CLASSIFIED INFORMATION

1. Classified Information shall be transmitted in accordance with the national laws and regulations of the Originating Party through diplomatic channels or as otherwise agreed in writing between the National Security Authorities.

2. The Parties may transmit Classified Information by electronic means in accordance with the security procedures approved by the National Security Authorities in writing.

ARTICLE 10
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. 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 Party.

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

4. Classified Information released under this Agreement marked „Szigorúan titkos!"/ SEGRETISSIMO/ TOP SECRET shall not be destroyed and shall be returned to the Originating Party.

5. In case of a crisis situation in which it is impossible to protect or to return the Classified Information to the Originating Party it shall be destroyed without undue delay. The National Security Authority of the Recipient Party shall notify the National Security Authority of the Originating Party in writing about the destruction of the Classified Information.

ARTICLE 11
VISITS

1. Visits requiring access to Classified Information shall be subject to the prior written consent of the National Security Authority of the respective Party.

2. The National Security Authority of the visiting Party shall notify the National Security Authority of the host Party about the planned visit through a request for visit 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 National Security Authorities.

3. The request 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 level and its validity;

d) date and duration of the visit, and 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 address of its point of contact;

g) date, signature and stamping of the official seal of the National Security Authority.

4. The National Security Authorities may agree on a list of visitors entitled to recurring visits. In case of projects or contracts which require recurring visits, the National Security Authorities of the Parties shall notify each other by sending a list of authorized personnel in accordance with national laws and regulations. Such list cannot be valid for more than twelve months. Once the list has been approved, visits may be arranged directly according to national laws and regulations.

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 any breach of security or suspicion thereof.

2. The National Security Authority of the Party where the breach of security has occurred, shall investigate the incident without undue delay. The National Security Authority of the other Party shall, if required, cooperate in the investigation.

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.

4. When the breach of security has occurred in a third Party, the National Security Authority which has released the Classified Information to the Third Party shall take the possible actions to ensure that the measures foreseen in this Article will be applied.

ARTICLE 13
EXPENSES

The implementation of this Agreement does not include any cost. Should any cost occur each Party shall bear its own costs.

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 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, without recourse to outside jurisdiction.

6. With the entry into force of this Agreement, the Agreement between the Government of the Republic of Hungary and the Government of the Italian Republic on the mutual protection of Classified Information signed on the 20th March 2003 shall expire.

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

Done in Budapest on November 26th, 2015 in two originals, in Hungarian, Italian and English languages, each text being equally authentic. In case of different interpretation the English text shall prevail.

For the Government of Hungary

For the Government of the Italian Republic”

4. §

(1) Ez a törvény – a (2) bekezdésben meghatározott kivétellel – a kihirdetését követő napon lép hatályba.
(2) A 2. §, a 3. § és a 6. § az Egyezmény 14. Cikk 1. bekezdésében meghatározott időpontban lép hatályba.
(3) Az Egyezmény, a 2. §, a 3. § és a 6. § 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.

6. §

Hatályát veszti a Magyar Köztársaság Kormánya és az Olasz Köztársaság Kormánya között a minősített információk kölcsönös védelméről szóló, Budapesten, 2003. március 20-án aláírt Biztonsági Megállapodás kihirdetéséről szóló 2004. évi LXXXIX. törvény.

Indokolás
a Magyarország Kormánya és az Olasz Köztársaság Kormánya között a minősített adatok cseréjéről és kölcsönös védelméről szóló egyezmény kihirdetéséről szóló törvényjavaslathoz

Általános indokolás

A két szerződő fél 2003-ban már kötött egy hasonló témájú megállapodást: a Magyar Köztársaság Kormánya és az Olasz Köztársaság Kormánya között a minősített információk kölcsönös védelméről szóló, Budapesten, 2003. március 20-án aláírt Biztonsági Megállapodást (a továbbiakban: Biztonsági Megállapodás), amelyet a 2004. évi LXXXIX. törvény hirdetett ki.

A Biztonsági Megállapodás új, a minősített adatok kölcsönös cseréjét és védelmét szabályozó egyezménnyel való felváltása azért szükséges, mert az Országgyűlés 2009. december 14-én elfogadta a minősített adat védelméről szóló 2009. évi CLV. törvényt, amely alapjaiban kodifikálta újra a minősített adatok védelmének magyarországi struktúráját.

A Biztonsági Megállapodás módosítására tehát a hatálybalépését követően eltelt időszakban bekövetkezett jogszabályi, valamint szervezeti változások miatt van szükség.

Az új Egyezmény a Biztonsági Megállapodással 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 a minősített szerződésekre, valamint a felek közötti látogatásokra. Míg a Biztonsági Megállapodás alapján a felek főszabály szerint diplomáciai úton érintkeztek, az új Egyezmény alapján a közvetlen információcsere válik általánossá. A megkötendő Egyezmény továbbá az átadó és átvevő fél kötelezettségeinek pontosabb meghatározását is tartalmazza, ezáltal bővítve a minősített adatok védelmére vonatkozó garanciális szabályok körét.

A bilaterális egyezmény szövegének megállapítására és a tárgyalások megkezdésére a felhatalmazást a minősített adatok kölcsönös védelméről szóló nemzetközi szerződések előkészítéséről és létrehozásáról szóló 58/2012. (V. 16.) ME határozat[1] adta meg.

[1] 58/2012. (V.16.) ME határozat a minősített adatok cseréjéről és kölcsönös védelméről szóló nemzetközi szerződések előkészítéséről és létrehozásáról a Magyarország Kormánya, valamint az Amerikai Egyesült Államok Kormánya, a Belga Királyság Kormánya, az Egyesült Királyság Kormánya, az Észt Köztársaság Kormánya, a Francia Köztársaság Kormánya, a Lett Köztársaság Kormánya, a Litván Köztársaság Kormánya, a Németországi Szövetségi Köztársaság Kormánya, az Olasz Köztársaság Kormánya, az Osztrák Köztársaság Kormánya, valamint a Svéd Királyság Kormánya között

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 jogi személyek és természetes személyek közötti együttműködés során kicserélt vagy keletkezett minősített adatok számára. Ennek keretében szabályozza a Felek közötti biztonsági együttműködést, kijelöli a hatáskörrel rendelkező hatóságokat, és rendelkezik egyes nemzeti minősítési szintek egymásnak történő megfeleltethetőségéről, valamint a minősített adat biztonságának megsértése esetén alkalmazandó eljárásról.

A 4. §-hoz

A Javaslat – a 2. §, a 3. § és a 6. § kivételével – a kihirdetését követő napon lép hatályba. A 2. §, a 3. § és a 6. § hatálybalépése az Egyezmény hatálybalépéséhez igazodik. Az Egyezmény „a Felek az Egyezmény hatálybalépéshez szükséges belső feltételek teljesítésére vonatkozó, diplomáciai úton küldött utolsó értesítése kézhezvételének napját követő második hónap első napján lép hatályba”. Ennek oka, hogy az Egyezmény kötelező hatályának elismerésére a Felek által alkalmazandó alkotmányos vagy belső jogi szabályokkal és eljárásokkal összhangban kerül sor. Az Egyezmény hatálybalépésének naptári napját a külpolitikáért felelős miniszter annak ismertté válását követően a Magyar Közlönyben közzétett egyedi közleményével állapítja meg.

Mivel az Egyezmény 14. cikkének 6. bekezdése hatályon kívül helyezi a felek között 2003-ban aláírt Biztonsági Megállapodást, a kihirdető törvény záró rendelkezései között szükséges rendelkezni a megállapodást kihirdető törvény hatályon kívül helyezéséről. A törvény hatályon kívül helyezésének napja megegyezik az Egyezmény hatálybalépésének napjával.

Az 5. §-hoz

E § rendelkezik arról, hogy a törvény végrehajtásához szükséges intézkedésekről a minősített adatok védelmének szakmai felügyeletéért felelős miniszter gondoskodik.

A 6. §-hoz

A Biztonsági Megállapodás új, a minősített adatok kölcsönös cseréjét és védelmét szabályozó egyezménnyel való felváltása azért szükséges, mert az Országgyűlés 2009. december 14-én elfogadta a minősített adat védelméről szóló 2009. évi CLV. törvényt, amely alapjaiban kodifikálta újra a minősített adatok védelmének magyarországi struktúráját.

A Biztonsági Megállapodás módosítására tehát a hatálybalépését követően eltelt időszakban bekövetkezett jogszabályi, valamint szervezeti változások miatt van szükség.

Az új Egyezmény a Biztonsági Megállapodással 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).