MAGYARORSZÁG KORMÁNYA

T/13090. számú

törvényjavaslat

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

Előadó: **Dr. Pintér Sándor**
belügyminiszter

Budapest, 2016. november

2016. évi … törvény

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

1. §

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

2. §

Az Országgyűlés az Egyezményt e törvénnyel kihirdeti.

3. §

Az Egyezmény hiteles magyar és angol nyelvű szövege a következő:

„EGYEZMÉNY MAGYARORSZÁG ÉS SPANYOLORSZÁG KÖZÖTT A MINŐSÍTETT ADATOK CSERÉJÉRŐL ÉS KÖLCSÖNÖS VÉDELMÉRŐL

Magyarország és Spanyolország (a továbbiakban együtt: „a Felek”),

Elismerve a Felek közötti kölcsönös együttműködés jelentőségét,

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

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

Kívánatosnak tartva, hogy a közöttük kicserélt minősített adatok megfelelő védelemben részesüljenek,

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 biztosítsa a Felek, vagy a joghatóságuk alá tartozó jogi személyek közötti együttműködés során kicserélt vagy keletkezett minősített adatok védelmét. Ezen rendelkezés azon természetes személyekre is vonatkozik, akik jelen Egyezmény értelmében minősített adathoz férnek hozzá.

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

2. CIKK

FOGALOMMEGHATÁROZÁSOK

Jelen Egyezmény alkalmazásában:

a) **„minősített adat biztonságának megsértése”** olyan tett vagy mulasztás, amely jelen Egyezménnyel vagy a Felek nemzeti jogszabályainak és egyéb szabályainak rendelkezéseivel ellentétes, és amely a minősített adat jogosulatlan nyilvánosságra hozatalát, elvesztését, megsemmisülését, jogosulatlan felhasználását vagy egyéb módon történő megsértését eredményezheti;

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

c) „**minősített adat”** megjelenési formájától függetlenül minden olyan adat, amelyet bármelyik Fél nemzeti jogszabályai és egyéb szabályai szerint védelemben kell részesíteni a minősített adat biztonságának megsértésével szemben, s amelyet ilyennek minősítettek;

d) **„szerződést kötő”** az a jogi személy, aki a minősített szerződés megkötésére a nemzeti jogszabályok és egyéb szabályok szerint jogképességgel rendelkezik;

e) **„telephely biztonsági tanúsítvány”** a nemzeti biztonsági hatóság azon pozitív döntése, amely szerint a létesítmény biztonsági szempontból nézve rendelkezik a minősített adatok kezeléséhez és tárolásához szükséges és a vonatkozó nemzeti jogszabályok és egyéb szabályok rendelkezéseinek megfelelő fizikai és szervezeti feltételekkel;

f) **„nemzeti biztonsági hatóság”** a Felek által kijelölt azon állami szervet jelenti, amely jelen Egyezmény végrehajtásáért és felügyeletéért felelős;

g) **„szükséges ismeret”** azt a követelményt jelenti, amely alapján meghatározott minősített adathoz való hozzáférés csak annak a személynek biztosítható, akinek az adott minősített adathoz való hozzáférés hivatali kötelessége vagy speciális feladata ellátásához igazoltan szükséges;

h) **„átadó fél”** azt a Felet, valamint a joghatósága alá tartozó jogi személyeket jelenti, amelyik a minősített adatot átadja;

i) **„személyi biztonsági tanúsítvány”** a nemzeti biztonsági hatóság azon pozitív döntése, amely szerint egy természetes személy a nemzeti jogszabályok és egyéb szabályok rendelkezéseinek tiszteletben tartásával jogosult hozzáférni minősített adatokhoz;

j) **„átvevő fél”** azt a Felet, valamint a joghatósága alá tartozó jogi személyeket jelenti, amelyik a minősített adatot átveszi.

k) **„harmadik fél”** bármely olyan államot, valamint a joghatósága alá tartozó jogi személyeket, továbbá nemzetközi szervezetet jelenti, amely nem részese jelen Egyezménynek.

3. CIKK

NEMZETI BIZTONSÁGI HATÓSÁGOK

(1) A Felek nemzeti biztonsági hatóságai a következők:

Magyarországon:

Nemzeti Biztonsági Felügyelet

Spanyolországban:

Államtitkár, a Nemzeti Hírszerzési Központ igazgatója
Nemzetbiztonsági Iroda

Secretario de Estado, Director del Centro Nacional de Inteligencia
Oficina Nacional de Seguridad

(2) A nemzeti biztonsági hatóságok egymás rendelkezésére bocsátják hivatalos elérhetőségeiket és tájékoztatják egymást az ezekkel kapcsolatos valamennyi későbbi változásról.

4. CIKK

MINŐSÍTÉSI SZINTEK MEGFELELTETÉSE ÉS JELÖLÉSEIK

Az egyes biztonsági minősítési szintek és jelöléseik az alábbiak szerint feleltethetők meg egymásnak:

Magyarországon	Spanyolországban
„Szigorúan titkos!”	SECRETO
„Titkos!”	RESERVADO
„Bizalmas!”	CONFIDENCIAL
„Korlátozott terjesztésű!”	DIFUSIÓN LIMITADA

5. CIKK

MINŐSÍTETT ADATHOZ VALÓ HOZZÁFÉRÉS

(1) Jelen Egyezmény alapján minősített adathoz való hozzáférésre az a személy jogosult, aki eleget tesz a szükséges ismeret elvének, és aki ezen adatokhoz való hozzáférésre az érintett Fél nemzeti jogszabályainak és egyéb szabályainak megfelelő felhatalmazást, valamint a minősített adat védelmére vonatkozó felelősségéről és kötelezettségeiről megfelelő tájékoztatást kapott.

(2) Azon természetes személyek, akik a minősített adathoz való hozzáférésre felhatalmazást kaptak, kötelesek jelen Egyezmény rendelkezésit betartani.

6. CIKK

A MINŐSÍTETT ADATOK VÉDELMÉRE VONATKOZÓ ALAPELVEK

(1) Az átadó fél:
a) biztosítja, hogy a minősített adaton a nemzeti jogszabályai és egyéb szabályai rendelkezéseinek megfelelő minősítési szint feltüntetésre kerüljön;
b) tájékoztatja az átvevő felet a minősített adat felhasználásával kapcsolatos esetleges feltételekről;
c) írásban haladéktalanul tájékoztatja az átvevő felet az adat minősítésében vagy a minősítés időtartamában bekövetkezett változásokról.

(2) Az átvevő fél:
a) biztosítja, hogy a minősített adaton feltüntetésre kerüljön a jelen Egyezmény 4. Cikke alapján meghatározott egyenértékű minősítési szint is;
b) ugyanolyan szintű védelemben részesíti a minősített adatot, mint amelyet a saját, azonos minősítési szintű nemzeti minősített adata számára biztosít;
c) biztosítja, hogy az átadó fél előzetes írásbeli hozzájárulása nélkül az átvett minősített adat minősítését nem szünteti meg, illetve 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, betartva az átadó fél által, a felhasználással kapcsolatban meghatározott esetleges feltételeket.

7. CIKK

BIZTONSÁGI EGYÜTTMŰKÖDÉS

(1) A hasonló szintű biztonsági követelmények fenntartása érdekében a nemzeti biztonsági hatóságok a másik fél megkeresésére tájékoztatják egymást a minősített adatok védelmével kapcsolatos nemzeti jogszabályokról és egyéb szabályokról, valamint mindezek gyakorlati alkalmazásáról.

(2) A Felek diplomáciai úton tájékoztatják egymást minden, a nemzeti jogszabályaikat és egyéb szabályaikat érintő, a nemzeti biztonsági hatóságok felelősségével kapcsolatos lényeges változásról.

(3) Megkeresés esetén a nemzeti biztonsági hatóságok, összhangban nemzeti jogszabályaik és egyéb szabályaik rendelkezéseivel, segítséget nyújtanak egymásnak a személyi biztonsági tanúsítványokkal és a telephely biztonsági tanúsítványokkal kapcsolatos eljárások során.

(4) A Felek megkeresés esetén nemzeti jogszabályaik és egyéb szabályaik rendelkezéseivel összhangban elismerik a másik Fél által kibocsátott személyi biztonsági tanúsítványokat és telephely biztonsági tanúsítványokat. Mindezek során a jelen Egyezmény 4. Cikkében foglaltak megfelelően alkalmazandók.

(5) A nemzeti biztonsági hatóságok haladéktalanul értesítik egymást az elismert személyi biztonsági tanúsítványaikkal és a telephely biztonsági tanúsítványaikkal kapcsolatos változásokról, különösen azok visszavonásáról.

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

8. CIKK

MINŐSÍTETT SZERZŐDÉSEK

(1) A minősített szerződéseket a Felek saját nemzeti jogszabályaik és egyéb szabályaik rendelkezései alapján kell megkötni és teljesíteni. A nemzeti biztonsági hatóságok megkeresésre megerősítik, hogy a szerződéskötést megelőző tárgyalásokban részt vevő lehetséges szerződést kötő vagy természetes személy, illetve a minősített szerződések teljesítésében részt vevő szerződést kötő vagy természetes személy rendelkezik-e a megfelelő személyi biztonsági tanúsítvánnyal vagy telephely biztonsági tanúsítvánnyal.

(2) Bármelyik Fél nemzeti biztonsági hatósága kérelmezheti biztonsági ellenőrzés lefolytatását a másik Fél országának területén működő létesítményben, a minősített adat folyamatos védelmének biztosítása céljából.

(3) A minősített szerződések részét képezi a minősített szerződés egyes elemeinek minősítési szintjével kapcsolatos biztonsági követelményeket tartalmazó projekt biztonsági utasítás, biztonsági szempontokra vonatkozó záradék vagy egyéb speciális biztonsági követelmény. A biztonsági követelmények másolatát azon Fél nemzeti biztonsági hatósága részére kell továbbítani, amelynek joghatósága alatt a minősített szerződés végrehajtása történik, ezáltal biztosítva a szerződést kötők által a minősített adat védelme érdekében kialakított biztonsági szabályok, eljárások és gyakorlat megfelelő hatóságét és ellenőrzését.

9. CIKK

A MINŐSÍTETT ADAT TOVÁBBÍTÁSA

(1) A minősített adat továbbítása az átadó fél nemzeti jogszabályainak és egyéb szabályainak rendelkezései szerint, diplomáciai úton, vagy a nemzeti biztonsági hatóságok által közösen, írásban meghatározott egyéb módon történik.

(2) A Felek a nemzeti biztonsági hatóságok által írásban jóváhagyott biztonsági 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 minimumra kell korlátozni.

(2) Jelen Egyezmény alapján átadott minősített adatról készült fordításokon a fordítás nyelvén fel kell tüntetni, hogy az átadó fél minősített adatát tartalmazza.

(3) Jelen Egyezmény alapján átadott „Szigorúan titkos!”/ SECRETO minősítésű adat fordítása vagy sokszorosítása kizárólag az átadó fél előzetes írásbeli engedélyével történhet.

(4) Jelen Egyezmény alapján átadott „Szigorúan titkos!”/ SECRETO minősítésű adat nem semmisíthető meg, és 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. A minősített adat megsemmisítésről az átvevő fél nemzeti biztonsági hatósága írásban értesíti az átadó fél nemzeti biztonsági hatóságát.

11. CIKK

LÁTOGATÁSOK

(1) Minősített adathoz való hozzáférést igénylő látogatásra a fogadó Fél nemzeti biztonsági hatóságának előzetes írásbeli jóváhagyása alapján kerülhet sor.

(2) A látogatást kezdeményező Fél nemzeti biztonsági hatósága látogatási kérelem formájában legalább húsz nappal a látogatás kezdő időpontja előtt értesíti a fogadó Fél nemzeti biztonsági hatóságát a tervezett látogatásról. Sürgős esetben, a nemzeti biztonsági hatóságok közötti előzetes egyeztetést követően a látogatási kérelem a látogatás kezdetéhez közelebbi időpontban is benyújtható.

(3) A látogatási kérelemnek legalább az alábbiakat kell tartalmaznia:

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

b) a látogató beosztásának és a látogató által képviselt intézmény megjelölése;

c) a látogató személyi biztonsági tanúsítványának szintje – amennyiben van ilyen – 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 minősített adatokat kezelő szervneve és címe, valamint a kapcsolattartójának neve, telefonszáma/ fax száma, e-mail címe;

g) dátum, aláírás és a nemzeti biztonsági hatóság hivatalos pecsétjének lenyomata.

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

(5) A fogadó Fél nemzeti biztonsági hatósága a látogatás jóváhagyását követően átadja a látogatási kérelem másolatát azon jogi személy hatáskörrel rendelkező biztonsági vezetőjének, amelynek a létesítményében a látogatásra sor kerül.

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

12. CIKK

A MINŐSÍTETT ADAT BIZTONSÁGÁNAK MEGSÉRTÉSE

(1) A nemzeti biztonsági hatóságok haladéktalanul írásban tájékoztatják egymást a minősített adat biztonságának bármilyen megsértéséről vagy annak gyanújáról.

(2) Annak a Félnek a nemzeti biztonsági hatósága, ahol a minősített adat biztonságának megsértése történt, haladéktalanul kivizsgálja az eseményt. A másik Fél nemzeti biztonsági hatósága szükség esetén részt vesz a vizsgálatban.

(3) Az átvevő fél nemzeti biztonsági hatósága minden esetben írásban tájékoztatja az átadó fél nemzeti biztonsági hatóságát a minősített adat biztonságának megsértésével kapcsolatos körülményekről, a kár mértékéről, a kár enyhítése érdekében megtett intézkedésekről, valamint a vizsgálat eredményéről.

13. CIKK

KÖLTSÉGEK VISELÉSE

(1) Főszabályként jelen Egyezmény végrehajtása nem jár költségekkel.

(2) Az esetlegesen mégis felmerülő költségek esetében, jelen Egyezmény végrehajtásával vagy felügyeletével összefüggésben felmerült költségeiket a Felek maguk viselik.

14. CIKK

ZÁRÓ RENDELKEZÉSEK

(1) Jelen Egyezmény határozatlan időre jön létre. Jelen Egyezmény a Felek által az Egyezmény hatálybalépéshez szükséges nemzeti jogi feltételek teljesítésére vonatkozó, diplomáciai úton küldött utolsó írásbeli értesítés kézhezvételének napját követő második hónap első napján lép hatályba.

(2) Jelen Egyezmény a Felek kölcsönös egyetértésével írásban bármikor módosítható. A módosítások hatálybalépésével kapcsolatban 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 hat hónap elteltével hatályát veszti.

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

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

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

Készült Budapesten, 2016. június 15-én, két eredeti példányban, magyar, spanyol és angol nyelven, valamennyi szöveg egyaránt hiteles. Értelmezésbeli eltérés esetén az angol nyelvű szöveg az irányadó.

……. ……..

Magyarország részéről Spanyolország részéről

AGREEMENT BETWEEN

HUNGARY AND SPAIN

ON THE EXCHANGE AND MUTUAL PROTECTION

OF CLASSIFIED INFORMATION

Hungary and Spain (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 that they ensure equivalent protection for the Classified Information,

Wishing to ensure the protection of Classified Information exchanged between them,

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 course of co-operation between the Parties or between the legal entities under their jurisdiction. This provision shall also apply to individuals who access Classified Information under the scope of this Agreement.

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

ARTICLE 2
DEFINITIONS

For the purpose of this Agreement:

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

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

c) **"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;

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

e) "**Facility Security Clearance**" means the positive determination granted by the National Security Authority that from a security point of view, a facility has the physical and organizational capability to handle and store Classified Information in accordance with the national laws and regulations;

f) "**National Security Authority**" means the state authority designated by a Party responsible for the application and supervision of this Agreement;

g) **"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;

h) **"Originating Party"** means the Party including the legal entities under its jurisdiction, which releases Classified Information;

i) "**Personnel Security Clearance**" means the positive determination granted by the National Security Authority that an individual is eligible to have access to Classified Information in accordance with the national laws and regulations;

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

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

ARTICLE 3
NATIONAL SECURITY AUTHORITIES

1. The National Security Authorities of the Parties are:

In Hungary:

National Security Authority

Nemzeti Biztonsági Felügyelet

In Spain:

Secretary of State, Director of the National Intelligence Centre

National Office of Security

Secretario de Estado, Director del Centro Nacional de Inteligencia

Oficina Nacional de Seguridad

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 Spain
„Szigorúan titkos!"	SECRETO
„Titkos!"	RESERVADO
„Bizalmas!"	CONFIDENCIAL
„Korlátozott terjesztésű!"	DIFUSIÓN LIMITADA

ARTICLE 5
ACCESS TO CLASSIFIED INFORMATION

1. Access to Classified Information under this Agreement shall be limited to individuals upon the Need-to-know principle, who are duly authorised in accordance with the national laws and

regulations of the respective Party and who are briefed on their responsibilities and obligations to protect Classified Information.

2. All individuals authorised to access Classified Information will be obliged to comply with the provisions of this Agreement.

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 conditions for the use of Classified Information;
c) inform the Recipient Party in writing without undue delay of any subsequent changes in the security classification level or duration of classification.

2. The Recipient Party shall:

a) ensure that Classified Information is also marked with the equivalent security classification marking in accordance with Article 4 of this Agreement;
b) afford the same degree of protection to Classified Information as afforded to its own Classified Information of the equivalent security 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 for which it has been released and in accordance with release conditions of the Originating Party.

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 their national laws and regulations concerning protection of Classified Information and the practices stemming from their implementation.

2. The Parties shall inform each other, through diplomatic channels, of any substantial change in national laws and regulations concerning the responsibilities of the National Security Authorities.

3. On request, the National Security Authorities shall, in accordance with their national laws and regulations, assist each other during the Personnel Security Clearance procedures and Facility Security Clearance procedures.

4. On request, 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. Article 4 of this Agreement shall apply accordingly.

5. The National Security Authorities shall promptly notify each other about changes in their respective Personnel Security Clearance certificates and Facility Security Clearance certificates, especially in case of their withdrawal.

6. Co-operation under this Agreement shall be effected in the English language.

ARTICLE 8
CLASSIFIED CONTRACTS

1. Classified Contracts shall be concluded and implemented in accordance with the national laws and regulations of each Party. On request, the National Security Authorities shall confirm that proposed contractors as well as individuals participating in pre-contractual negotiations or in the implementation of Classified Contracts have the appropriate Personnel Security Clearance certificate or Facility Security Clearance certificate.

2. The National Security Authority of either Party may request that a security inspection is carried out at a facility located on the territory of the other Party to ensure continuing protection of Classified Information.

3. Classified Contracts shall contain security requirements on the security classification level of each element of the Classified Contract in the form of Programme Security Instructions, Security Aspects Letter or other specific security requirements. A copy of the security requirements shall be forwarded to the National Security Authority of the Party under whose jurisdiction the Classified Contract is to be implemented, to allow adequate supervision and control of the security standards, procedures and practices established by the Contractors for the protection of Classified Information.

ARTICLE 9
TRANSFER AND TRANSMISSION OF CLASSIFIED INFORMATION

1. Classified Information shall be transferred 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. 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 Party.

3. Classified Information released under this Agreement marked „Szigorúan titkos!”/SECRETO shall be translated or reproduced only with the prior written consent of the Originating Party.

4. Classified Information released under this Agreement marked „Szigorúan titkos!”/SECRETO / 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 host 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 shorter notice, subject to prior co-ordination between the National Security Authorities.

3. The request for visit shall contain as a minimum:

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 status when appropriate, 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. The National Security Authorities shall agree on the further details of the recurring visits.

5. Once the visit has been approved, the National Security Authority of the host Party shall provide a copy of the request for visit to the competent security officer of the legal entity whose facilities are to be visited.

6. 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, co-operate in the investigation.

3. In all cases, 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

1. In principle, the implementation of this Agreement shall not generate any costs.

2. In the case of any cost, each Party shall bear its own expenses incurred in the course of the implementation of this Agreement and its supervision.

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 written notification 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 at any time 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 denounce 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 denunciation.

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 unless 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.

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

Done in Budapest on 15th June 2016 in two originals, in Hungarian, Spanish and English languages, each text being equally authentic. In case of different interpretation the English text shall prevail.

For Hungary **For Spain”**

4. §

(1) Ez a törvény – a (2) bekezdésben meghatározott kivétellel – a kihirdetését követő napon lép hatályba.
(2) A 2. § és a 3. § az Egyezmény 14. cikk (1) bekezdésében meghatározott időpontban lép hatályba.
(3) Az Egyezmény, illetve a 2. § és a 3. § hatálybalépésének naptári napját a külpolitikáért felelős miniszter annak ismertté válását követően a Magyar Közlönyben haladéktalanul közzétett közleményével állapítja meg.
(4) Az e törvény végrehajtásához szükséges intézkedésekről a minősített adatok védelmének szakmai felügyeletéért felelős miniszter gondoskodik.

Indokolás a Magyarország Kormánya és a Spanyol Királyság Kormánya között a minősített adatok cseréjéről és kölcsönös védelméről szóló egyezmény kihirdetéséről szóló törvényjavaslathoz

Általános indokolás

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

A minősített adatok cseréjére vonatkozó biztonsági együttműködés érdekében – a katonai megállapodások kivételével – hazánk jogszabályi felhatalmazás hiányában korábban csak két állammal kötött általános titokvédelmi egyezményt (*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. törvény, valamint a Magyar Köztársaság Kormánya és Német 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),* 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.

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 kötött hasonló megállapodást, valamint az 54/2013. ME határozat alapján 2014. július 3-án a Macedón Köztársaság és Magyarország, 2014. szeptember 8-án az Albán Köztársaság és Magyarország között jött létre a minősített adatok cseréjéről és kölcsönös védelméről szóló egyezmény. Az 58/2012. (V. 16.) ME határozat alapján létrehozásra került a Belga Királyság és Magyarország közötti megállapodás, amelynek aláírására 2015. szeptember 21-én került sor, az 54/2013. (IV. 16.) ME határozat alapján pedig a Ciprusi Köztársaság és Magyarország közötti megállapodás jött létre, amelynek aláírására 2015. október 29-én került sor. 2015. november 25-én aláírásra került az 58/2012. (V. 16.) ME határozat alapján létrehozott megállapodás Magyarország és az Olasz Köztársaság között. Az 54/2013. (IV. 10.) ME határozat alapján 2016-ban négy

megállapodás aláírására került sor; 2016. január 22-én a Szlovén Köztársasággal, 2016. június 10-én a Horvát Köztársasággal, 2016. október 6-án Montenegróval.

2016. június 15-én, Budapesten került sor *a Magyarország Kormánya és Spanyolország között a minősített adatok cseréjéről és kölcsönös védelméről szóló egyezmény* (a továbbiakban: Egyezmény) aláírására, amelyre *a Magyarország Kormánya és Spanyolország között a minősített adatok cseréjéről és kölcsönös védelméről szóló egyezmény szövegének végleges megállapítására adott felhatalmazásról szóló 1884/2015. (XII. 2.) Korm. határozat* adott felhatalmazást.

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

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. és 3. § kivételével – a kihirdetését követő napon lép hatályba. A 2. § és 3. § hatálybalépése az Egyezmény hatálybalépéséhez igazodik. Az Egyezmény „a Feleknek az Egyezmény hatálybalépéshez szükséges belső jogi feltételek teljesítésére vonatkozó, diplomáciai úton küldött utolsó, írásbeli 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.