MAGYARORSZÁG KORMÁNYA

T/17298. számú

törvényjavaslat

a Magyarország Kormánya és a Bolgár 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 a Bolgár 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 Bolgár 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 BOLGÁR KÖZTÁRSASÁG KORMÁNYA KÖZÖTT
A MINŐSÍTETT ADATOK CSERÉJÉRŐL ÉS KÖLCSÖNÖS VÉDELMÉRŐL

Magyarország Kormánya és a Bolgár Köztársaság Kormánya (a továbbiakban: 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 vagy a joghatóságuk alá tartozó jogi személyek és természetes személyek között kicserélt minősített adatok védelemben részesüljenek,

Kölcsönösen tiszteletben tartva a nemzeti érdekeket és a biztonságot, 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 során kicserélt vagy keletkezett minősített adatok számára.

(2) Jelen Egyezmény nem érinti a Felek azon kötelezettségeit, amelyek más kétoldalú vagy többoldalú megállapodás alapján keletkeztek, beleértve valamennyi, a minősített adat cseréjéről és kölcsönös védelméről szóló egyezményt.

2. CIKK

FOGALOMMEGHATÁROZÁSOK

Jelen Egyezmény alkalmazásában:

a) **minősített adat**: megjelenési formájától vagy természetétől függetlenül, minden olyan adat, amelyet bármelyik Fél nemzeti jogszabályainak és egyéb szabályainak rendelkezései szerint védelemben kell részesíteni a minősített adat biztonságának megsértésével szemben, és amelyen a minősítési szint feltüntetésre került;
b) **minősítési szint:** az a kategória, amely a nemzeti jogszabályok és egyéb szabályok rendelkezései alapján a minősített adat fontosságának mértékére, az adathoz történő hozzáférés korlátozásának fokára és a Felek által teljesítendő védelem szintjére utal;
c) **minősített adat biztonságának megsértése**: olyan, jelen Egyezménnyel vagy a Felek nemzeti jogszabályaival és egyéb szabályainak rendelkezéseivel ellentétes tevékenység vagy mulasztás, ami a minősített adat nyilvánosságra hozatalához, elvesztéséhez, megsemmisüléséhez, jogosulatlan felhasználásához vagy egyéb módon történő megsértéséhez vezethet;
d) **minősített szerződés**: olyan szerződés, amely minősített adatot tartalmaz, vagy amely alapján minősített adathoz való hozzáférés szükséges;
e) **szerződő**: olyan természetes személy vagy jogi személy, amely a nemzeti jogszabályok és egyéb szabályok rendelkezéseivel összhangban rendelkezik a minősített szerződések megkötésére irányuló jogképességgel;
f) **alvállalkozó:** olyan természetes személy vagy jogi személy, amely rendelkezik a minősített szerződések megkötésére irányuló jogképességgel, és amely a szerződővel alvállalkozói szerződést köt;
g) **telephely biztonsági tanúsítvány**: a hatáskörrel rendelkező hatóság azon döntése, amely megállapítja, hogy a jogképességgel rendelkező jogi személy a nemzeti jogszabályokkal és egyéb szabályok rendelkezéseivel összhangban rendelkezik a minősített adatok kezelésére és tárolására vonatkozó fizikai és szervezeti képességekkel;
h) **személyi biztonsági tanúsítvány**: a hatáskörrel rendelkező hatóság azon döntése, amely megállapítja, hogy a természetes személy a nemzeti jogszabályokkal és egyéb szabályok rendelkezéseivel összhangban hozzáférhet minősített adatokhoz;
i) **szükséges ismeret**: az a követelmény, amely alapján meghatározott minősített adathoz való hozzáférés csak annak a személynek biztosítható, akinek az adott minősített adathoz való hozzáférés hivatali kötelessége vagy meghatározott feladata ellátásához igazoltan szükséges;
j) **nemzeti biztonsági hatóság:** az az állami szerv, amely jelen Egyezmény alkalmazásáért és felügyeletéért felelős;
k) **átadó fél:** az a Fél, beleértve a joghatósága alá tartozó jogi személyeket vagy természetes személyeket, amelyik a minősített adatot átadja;
l) **átvevő fél:** az a Fél, beleértve a joghatósága alá tartozó jogi személyeket vagy természetes személyeket, amelyik a minősített adatot átveszi;

m)**harmadik fél**: bármely olyan állam, beleértve a joghatósága alá tartozó jogi személyeket vagy természetes személyeket, vagy nemzetközi szervezet, amely nem részese jelen Egyezménynek.

3. CIKK

NEMZETI BIZTONSÁGI HATÓSÁGOK

(1) A Felek nemzeti biztonsági hatóságai:

Magyarországon:

- Nemzeti Biztonsági Felügyelet

(National Security Authority)

A Bolgár Köztársaságban:

- Állami Információbiztonsági Bizottság

(Държавна комисия по сигурността на информацията)

(2) A nemzeti biztonsági hatóságok tájékoztatják egymást hivatalos elérhetőségi adataikról és az azokban bekövetkezett valamennyi későbbi változásról.

4. CIKK

MINŐSÍTÉSI SZINTEK

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

Magyarországon	**A Bolgár Köztársaságban**	**Angol nyelvű megfelelőjük**
„Szigorúan titkos!”	СТРОГО СЕКРЕТНО	TOP SECRET
„Titkos!”	СЕКРЕТНО	SECRET
„Bizalmas!”	ПОВЕРИТЕЛНО	CONFIDENTIAL
„Korlátozott terjesztésű!”	ЗА СЛУЖЕБНО ПОЛЗВАНЕ	RESTRICTED

5. CIKK

MINŐSÍTETT ADATHOZ VALÓ HOZZÁFÉRÉS

Jelen Egyezmény alapján minősített adathoz kizárólag olyan természetes személyek kaphatnak hozzáférést, akik a szükséges ismeret elvének megfelelnek, és akik az érintett Fél nemzeti jogszabályaival és egyéb szabályainak rendelkezéseivel összhangban erre megfelelő felhatalmazást kaptak.

6. CIKK

ALAPVETŐ BIZTONSÁGI KÖVETELMÉNYEK

(1) Az átadó fél:

a) biztosítja, hogy a minősített adaton a nemzeti jogszabályai és egyéb szabályainak rendelkezései szerinti megfelelő minősítési szint feltüntetésre kerüljön;
b) tájékoztatja az átvevő Felet a minősített adat felhasználásával kapcsolatos esetleges feltételekről;
c) késedelem nélkül írásban tájékoztatja az átvevő Felet az adat minősítési szintjében vagy a minősítés időtartamában bekövetkezett későbbi változásokról.

(2) Az átvevő fél:

a) biztosítja, hogy a minősített adaton feltüntetésre kerüljön jelen Egyezmény 4. cikke alapján meghatározott egyenértékű minősítési szint;
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 minősítése nem kerül megszüntetésre, valamint minősítési szintje megváltoztatásra az átadó fél előzetes, írásbeli hozzájárulása nélkül;
d) biztosítja, hogy az átadó fél előzetes írásbeli hozzájárulása nélkül a 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 meghatározott kezelési előírásokat.

7. CIKK

BIZTONSÁGI EGYÜTTMŰKÖDÉS

(1) Az összeegyeztethető szintű biztonsági követelmények fenntartása érdekében a nemzeti biztonsági hatóságok megkeresésre tájékoztatják egymást a minősített adat védelmével kapcsolatos nemzeti jogszabályokról és egyéb szabályokról, valamint mindezek gyakorlati alkalmazásáról. A nemzeti biztonsági hatóságok értesítik egymást a minősített adatok védelmét érintő nemzeti jogszabályaikban és egyéb szabályaikban bekövetkezett azon jelentős változásokról, melyek jelen Egyezmény végrehajtását érintik.

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

(3) Megkeresés esetén a Felek nemzeti jogszabályaikkal és egyéb szabályaikkal összhangban elismerik a másik Fél által kibocsátott személyi biztonsági tanúsítványokat és telephely biztonsági tanúsítványokat. Jelen Egyezmény 4. cikkében foglaltak megfelelően alkalmazandók.

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

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

8. CIKK

MINŐSÍTETT SZERZŐDÉSEK

(1) A minősített szerződéseket a Felek saját nemzeti jogszabályai és egyéb szabályainak rendelkezései alapján kell megkötni és teljesíteni. A nemzeti biztonsági hatóságok megkeresésre megerősítik, hogy a lehetséges szerződők, valamint a szerződéskötést megelőző tárgyalásokban vagy a minősített szerződések teljesítésében részt vevő természetes személyek rendelkeznek megfelelő személyi biztonsági tanúsítvánnyal vagy telephely biztonsági tanúsítvánnyal.

(2) A nemzeti biztonsági hatóság felkérheti a másik Fél nemzeti biztonsági hatóságát biztonsági ellenőrzés lefolytatására a másik Fél területén működő létesítményben, a minősített adatok folyamatos védelmének biztosítása céljából.

(3) A nemzeti jogszabályok és egyéb szabályok rendelkezései alapján a minősített szerződés részét képezi a biztonsági követelményeket megfogalmazó melléklet. A biztonsági követelményeket megfogalmazó melléklet másolatát azon Fél nemzeti biztonsági hatósága részére kell továbbítani, amelynek joghatósága alatt a minősített szerződés teljesítése történik.

(4) A biztonsági követelményeket megfogalmazó melléklet a nemzeti jogszabályok és egyéb szabályok rendelkezéseivel összhangban legalább a következőket tartalmazza:

a) minősítési útmutató;
b) az adat minősítési szintjében bekövetkezett változásokról történő tájékoztatás menetének leírása;
c) kommunikációs csatornák;
d) a minősített adat továbbításának menete;
e) a szerződéssel érintett minősített adat védelmének koordinálásáért felelős nemzeti biztonsági hatóságok elérhetőségi adatai;
f) értesítési kötelezettség a minősített adat biztonságának bekövetkezett vagy gyanított megsértése esetén.

(5) Az alvállalkozók kötelesek ugyanazon biztonsági követelményeknek eleget tenni, mint a szerződő.

9. CIKK

A MINŐSÍTETT ADAT TOVÁBBÍTÁSA

(1) A minősített adat továbbítása az átadó fél nemzeti jogszabályaival és egyéb szabályainak rendelkezéseivel összhangban diplomáciai úton, vagy a nemzeti biztonsági hatóságok által 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.

(3) Minősített adatot tartalmazó nagyméretű küldemény továbbítása esetén a nemzeti biztonsági hatóságok kölcsönösen megállapodnak a továbbítás módjáról, az útvonalról és az egyéb biztonsági intézkedésekről.

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 szintet és az adatot úgy kell védeni, 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!”/ СТРОГО СЕКРЕТНО/ TOP SECRET minősítésű adat fordítása vagy sokszorosítása kizárólag az átadó Fél előzetes írásbeli hozzájárulásával lehetséges.

(4) A minősített adatot oly módon kell megsemmisíteni, hogy annak helyreállítása se részben, se egészben ne legyen lehetséges.

(5) Jelen Egyezmény alapján átadott „Szigorúan titkos!”/ СТРОГО СЕКРЕТНО/ TOP SECRET minősítésű adat nem semmisíthető meg és az átadó félnek vissza kell szolgáltatni.

(6) A minősített adatot olyan válsághelyzet esetén, amely lehetetlenné teszi a védelmét, vagy ha az átadó félhez való visszajuttatása nem lehetséges, késedelem nélkül meg kell semmisíteni. A minősített adat megsemmisítéséről az átvevő fél nemzeti biztonsági hatósága írásban értesíti az átadó fél nemzeti biztonsági hatóságát.

11. CIKK

LÁTOGATÁSOK

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

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

(3) A látogatási kérelem az alábbiakat tartalmazza:

a) a látogató neve, születési ideje és helye, állampolgársága, útlevelének vagy más személyazonosító igazolványának száma;
b) a látogató beosztásának és a látogató által képviselt szervezeti egységnek 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 minősített adatokat kezelő szerv neve és címe, valamint a kapcsolattartójának neve, telefonszáma, faxszáma, 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 részleteiről a nemzeti biztonsági hatóságok kötelesek megállapodni.

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

12. CIKK

A MINŐSÍTETT ADAT BIZTONSÁGÁNAK MEGSÉRTÉSE

(1) A nemzeti biztonsági hatóságok haladéktalanul írásban tájékoztatják egymást a minősített adat biztonságának megsértéséről, vagy ha mindezek gyanúja merül fel.

(2) Azon Fél nemzeti biztonsági hatósága, ahol a minősített adat biztonságának megsértésére sor került, nemzeti jogszabályaival és egyéb szabályaival összhangban haladéktalanul kivizsgálja a minősített adat megsértését vagy annak kivizsgálásának kezdeményezéséről gondoskodik. A másik Fél nemzeti biztonsági hatósága szükség esetén közreműködik a vizsgálatban.

(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.

(4) Ha a minősített adat biztonságának megsértése harmadik államban következik be, az adatot továbbító Fél nemzeti biztonsági hatósága lehetőség szerint megteszi a jelen cikk (2) pontjában előírt intézkedéseket.

13. CIKK

KÖLTSÉGEK

A Felek maguk viselik jelen Egyezmény végrehajtásával összefüggésben felmerült költségeiket.

14. CIKK

ZÁRÓ RENDELKEZÉSEK

(1) Jelen Egyezmény határozatlan időre jön létre. Jelen Egyezmény a Felek az Egyezmény hatálybalépéshez szükséges nemzeti, jogi 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 kézhezvételének napjától számított hat hónap elteltével hatályát veszti.

(4) Az Egyezmény megszűnésétől függetlenül jelen Egyezmény alapján kicserélt vagy keletkezett valamennyi minősített adatot 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) Jelen Egyezmény értelmezéséből vagy végrehajtásából fakadó vitákat a Felek egymás között egyeztetés és tárgyalás útján, külső igazságszolgáltatási fórum igénybevétele nélkül rendezik.

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

Készült Szófiában, 2017. július 5-én, két eredeti példányban, magyar, bolgár és angol nyelven, valamennyi szöveg egyaránt hiteles. Eltérő értelmezés esetén az angol nyelvű szöveg az irányadó.

Magyarország Kormánya részéről **A Bolgár Köztársaság Kormánya részéről”**

”AGREEMENT

BETWEEN THE GOVERNMENT OF HUNGARY AND THE GOVERNMENT OF THE REPUBLIC OF BULGARIA ON THE EXCHANGE AND MUTUAL PROTECTION OF CLASSIFIED INFORMATION

The Government of Hungary and the Government of the Republic of Bulgaria (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 or between the legal entities and individuals under their jurisdiction,

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 and individuals under their jurisdiction.

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) **“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 to which a security classification level has been attributed;
b) **“Security classification level”** means a category, according to the national laws and regulations, which characterises the importance of the Classified Information, the level of restriction of access to it and the level of its protection by the Parties;
c) **“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;
d) **“Classified Contract”** means a contract that involves or requires access to Classified Information;
e) **“Contractor**” means an individual or a legal entity possessing the legal capacity to conclude

Classified Contracts in accordance with the national laws and regulations;
f) **"Subcontractor"** means an individual or a legal entity possessing the legal capacity to conclude Classified Contracts, to whom a Contractor lets a subcontract;
g) "**Facility Security Clearance**" means the determination by the respective competent authority that a legal entity, possessing the legal capacity, has the physical and organizational capability to handle and store Classified Information in accordance with the national laws and regulations;
h) "**Personnel Security Clearance**" means the determination by the respective competent authority that an individual is eligible to have access to Classified Information in accordance with the national laws and regulations;
i) **"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;
j) "**National Security Authority**" means the state authority responsible for the application and supervision of this Agreement;
k) **"Originating Party"** means the Party including the legal entities or individuals under its jurisdiction, which releases Classified Information;
l) **"Recipient Party"** means the Party including the legal entities or individuals under its jurisdiction, which receives Classified Information;
m)**"Third Party"** means any state including the legal entities or individuals under its jurisdiction or international organisation not being a Party to 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 Republic of Bulgaria:

- Държавна комисия по сигурността на информацията

(State Commission on Information Security)

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

The equivalence of national security classification levels is as follows:

For Hungary	For the Republic of Bulgaria	Equivalent in English language
„Szigorúan titkos!"	СТРОГО СЕКРЕТНО	TOP SECRET

„Titkos!”	СЕКРЕТНО	SECRET
„Bizalmas!”	ПОВЕРИТЕЛНО	CONFIDENTIAL
„Korlátozott terjesztésű!”	ЗА СЛУЖЕБНО ПОЛЗВАНЕ	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 authorised in accordance with the national laws and regulations of the respective Party.

ARTICLE 6
BASIC SECURITY REQUIREMENTS

1. The Originating Party shall:
a) ensure that Classified Information is marked with appropriate security classification level 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 or duration of classification.

2. The Recipient Party shall:
a) ensure that Classified Information is marked with equivalent security classification level 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 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 it has been released for and in accordance with the 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. The National Security Authorities shall inform each other of any substantive changes of their national laws and regulations in the field of protection of Classified Information concerning the implementation of this Agreement.

2. 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.

3. On request, the Parties shall, in accordance with their national laws and regulations, recognise the Personnel Security Clearances and Facility Security Clearances of the other Party. Article 4 of this Agreement shall apply accordingly.

4. The National Security Authorities shall promptly notify each other about changes in the recognised Personnel Security Clearances and Facility Security Clearances, especially in case of their withdrawal.

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

ARTICLE 8
CLASSIFIED CONTRACTS

1. Classified Contracts shall be concluded and implemented in accordance with the national laws and regulations of each Party. On request, the 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 appropriate Personnel Security Clearance or Facility Security Clearance.

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

3. Classified Contracts shall contain an appropriate section on the security requirements in accordance with the national laws and regulations. A copy of the section on the security requirements shall be forwarded to the National Security Authority of the Party under whose jurisdiction the Classified Contract is to be implemented.

4. The section on the security requirements, in accordance with the national laws and regulations shall include at least the following aspects:

a) a classification guide;
b) a procedure for the communication of changes in the security classification level of the information;
c) communication channels;
d) procedures for the transportation of Classified Information;
e) contact details of the National Security Authorities responsible for the co-ordination of the protection of Classified Information related to the Contract;
f) the procedure for notification of any breach of security or suspicion thereof.

5. All subcontractors shall fulfil the same security obligations as the Contractor.

ARTICLE 9
TRANSFER OR 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.

3. In case of transferring a large consignment containing Classified Information, the National Security Authorities shall mutually agree on and approve the means of transportation, the route and the other security measures.

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 level 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!”/ СТРОГО СЕКРЕТНО/ TOP SECRET shall be translated or reproduced only upon the prior written consent of the Originating Party.

4. Classified Information shall be destroyed insofar as to prevent its reconstruction in whole or in part.

5. Classified Information released under this Agreement marked „Szigorúan titkos!”/ СТРОГО СЕКРЕТНО/ TOP SECRET shall not be destroyed and shall be returned to the Originating Party.

6. 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 organizational entity represented;
c) visitor's Personnel Security Clearance 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. The National Security Authorities 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 any breach of security or suspicion thereof.

2. The National Security Authority of the Party where the breach of security has occurred, shall investigate or initiate an investigation of the incident without undue delay, according to the national laws and regulations. The National Security Authority of the other Party shall, if required, co-operate 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. In case a breach of security occurs in a third country, the National Security Authority of the transferring Party shall take the actions under paragraph 2, where possible.

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 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.

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

Done in Sofia on the 5th of July 2017, in two originals, in Hungarian, Bulgarian 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 Republic of Bulgaria”**

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 BOLGÁR 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 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 minősített adat védelméről szóló 2009. évi CLV. törvény 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.

A Mavtv-ben foglaltak végrehajtása, Magyarország nemzetközi kötelezettségvállalásainak teljesítése, továbbá a minősített adatok cseréjével és kölcsönös védelmével történő szorosabb együttműködés biztosítása miatt kiemelt jelentőségű a ME határozatokban megjelölt további országokkal az egyezménytervezetek előkészítése. Ennek érdekében került sor a Magyarország Kormánya és a Bolgár Köztársaság Kormánya között a minősített adatok cseréjéről és kölcsönös védelméről szóló egyezmény létrehozására, amelyet a felek 2017. június 28-án , Szófiában írtak alá.

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 a 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 a 3. § kivételével a kihirdetését követő napon lép hatályba. A 2. § és a 3. § hatálybalépése az Egyezmény hatálybalépéséhez igazodik. Az Egyezmény 14. Cikk 1. bekezdése szerint az Egyezmény „a Felek az Egyezmény hatálybalépéshez szükséges nemzeti, jogi 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 kerüljön sor. Az Egyezmény hatálybalépésének naptári napját a külpolitikáért felelős miniszter annak ismertté válását követően a Magyar Közlönyben közzétett egyedi közleményével állapítja meg.