MAGYARORSZÁG KORMÁNYA

T/13086. számú

törvényjavaslat

a Magyarország Kormánya és a Horvát Köztársaság 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 Horvát 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 Horvát 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 HORVÁT KÖZTÁRSASÁG KORMÁNYA KÖZÖTT A MINŐSÍTETT ADATOK CSERÉJÉRŐL ÉS KÖLCSÖNÖS VÉDELMÉRŐL

Magyarország Kormánya és a Horvát 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 megfelelő 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 joghatóságuk alá tartozó jogi személyek vagy természetes személyek közötti együttműködés során keletkezett vagy kicserélt 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 kivéve, ha jelen Egyezmény szigorúbb szabályokat állapít meg a minősített adatok cseréjére vagy kölcsönös védelmére.

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 amelyet ennek megfelelően minősítettek és minősítési jelöléssel láttak el;

b) **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 szükséges;

c) **minősítési szint:** az a kategória, amely a nemzeti jogszabályok és egyéb szabályok rendelkezéseivel összhangban a minősített adathoz való hozzáférés korlátozásának szintjét és a védelem legkisebb szintjét jelöli;

d) **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 bizalmasságának, sérthetetlenségének vagy rendelkezésre állásának egyéb módon történő megsértéséhez vezethet;

e) **Átadó Fél:** az a Fél – beleértve a joghatósága alá tartozó jogi személyeket vagy természetes személyeket –, amelyik a minősített adatot átadja;

f) **Átvevő Fél:** az a Fél – beleértve a joghatósága alá tartozó jogi személyeket vagy természetes személyeket –, amelyik a minősített adatot átveszi;

g) **nemzeti biztonsági felügyelet:** az az állami szerv, amely jelen Egyezmény végrehajtásáért és felügyeletéért felelős;

h) **személyi biztonsági tanúsítvány**: a nemzeti biztonsági felügyelet azon döntése, amely megállapítja, hogy egy személy a nemzeti jogszabályok és egyéb szabályok rendelkezéseivel összhangban hozzáférhet minősített adatokhoz;

i) **telephely biztonsági tanúsítvány**: a nemzeti biztonsági felügyelet azon döntése, amely megállapítja, hogy a jogképességgel rendelkező jogi személy a nemzeti jogszabályok és egyéb szabályok rendelkezéseivel összhangban rendelkezik a minősített adatok kezelésére és tárolására vonatkozó fizikai és szervezeti képességekkel;

j) **minősített szerződés**: olyan szerződés, amely minősített adatot tartalmaz, vagy amely alapján minősített adathoz való hozzáférés szükséges;

k) **szerződő**: olyan természetes személy vagy jogi személy, aki a nemzeti jogszabályok és egyéb szabályok rendelkezéseivel összhangban rendelkezik a minősített szerződések megkötésére irányuló képességgel;

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

3. CIKK

NEMZETI BIZTONSÁGI FELÜGYELETEK

(1) A Felek nemzeti biztonsági felügyeletei:

Magyarországon:
Nemzeti Biztonsági Felügyelet

A Horvát Köztársaságban:
Ured Vijeća za nacionalnu sigurnost (A Nemzeti Biztonsági Tanács Hivatala)

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

(3) A Felek diplomáciai úton tájékoztatják egymást a nemzeti biztonsági felügyeletekkel kapcsolatos valamennyi későbbi változásról.

4. CIKK

MINŐSÍTÉSI SZINTEK ÉS JELÖLÉSEK

(1) Jelen Egyezmény alapján keletkezett vagy kicserélt valamennyi minősített adatot a Felek nemzeti jogszabályai és egyéb szabályai szerint, a megfelelő minősítési jelöléssel kell ellátni.

(2) Az egyes nemzeti minősítési szintek és jelölések az alábbiak szerint feleltethetők meg egymásnak:

Magyarországon	**A Horvát Köztársaságban**	**Angol nyelvű megfelelőjük**
„Szigorúan titkos!”	VRLO TAJNO	TOP SECRET
„Titkos!”	TAJNO	SECRET
„Bizalmas!”	POVJERLJIVO	CONFIDENTIAL
„Korlátozott terjesztésű!”	OGRANIČENO	RESTRICTED

5. CIKK

MINŐSÍTETT ADATHOZ VALÓ HOZZÁFÉRÉS

Jelen Egyezmény alapján minősített adathoz kizárólag olyan személyek kaphatnak hozzáférést, akik a szükséges ismeret elvének megfelelnek, és akik a nemzeti jogszabályok és egyéb szabályok rendelkezéseinek megfelelően rendelkeznek személyi biztonsági tanúsítvánnyal és tájékoztatást kaptak a minősített adatok védelmével kapcsolatos kötelezettségeikről.

6. CIKK

BIZTONSÁGI ALAPELVEK

(1) Jelen Egyezmény alapján keletkezett vagy kicserélt minősített adatok védelme érdekében a Felek nemzeti jogszabályaik és egyéb szabályaik rendelkezéseivel összhangban minden szükséges intézkedést megtesznek.

(2) Az Átadó Fél:
a) biztosítja, hogy a minősített adaton a nemzeti jogszabályok és egyéb szabályok 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 minősítésében vagy a minősítés érvényességi idejében bekövetkezett későbbi változásokról.

(3) Az Átvevő Fél:
a) biztosítja, hogy a minősített adaton jelen Egyezmény 4. cikke alapján meghatározott egyenértékű minősítési szint kerüljön feltüntetésre;
b) ugyanolyan szintű védelemben részesíti a minősített adatot, mint amelyet a saját, jelen Egyezmény 4. cikke alapján azonos minősítési szintű nemzeti minősített adata számára biztosít;
c) biztosítja, hogy a minősített adat minősítését nem szünteti meg, valamint a minősítési szintjét nem változtatja meg 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 felügyeletek megkeresésre tájékoztatják egymást a minősített adat védelmével kapcsolatos nemzeti jogszabályokról és egyéb szabályokról, valamint mindezek gyakorlati alkalmazásáról. A nemzeti biztonsági felügyeletek tájékoztatják egymást a minősített adatokkal kapcsolatos nemzeti jogszabályaikban és egyéb szabályaikban bekövetkezett valamennyi későbbi változásról.

(2) Megkeresés esetén a nemzeti biztonsági felügyeletek a nemzeti jogszabályok és egyéb szabályok rendelkezéseivel összhangban segítséget nyújtanak egymásnak a személyi biztonsági tanúsítványok és a telephely biztonsági tanúsítványokkal kapcsolatos eljárások során.

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

(4) A nemzeti biztonsági felügyeletek 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 jogszabályainak és egyéb szabályainak rendelkezései alapján kell megkötni és teljesíteni. A nemzeti biztonsági felügyeletek megkeresésre megerősítik, hogy a lehetséges szerződő, valamint a szerződéskötést megelőző tárgyalásokban részt vevő vagy a „Bizalmas!" / POVJERLJIVO / CONFIDENTIAL vagy magasabb szintű minősített szerződések teljesítésében részt vevő természetes személyek rendelkeznek megfelelő személyi biztonsági tanúsítvánnyal vagy telephely biztonsági tanúsítvánnyal.

(2) Amennyiben a lehetséges szerződő nem rendelkezik megfelelő biztonsági tanúsítvánnyal, az Átadó Fél nemzeti biztonsági felügyelete kérelmezheti az Átvevő Fél nemzeti biztonsági felügyeleténél a megfelelő biztonsági tanúsítvány kiállítását.

(3) Bármelyik Fél nemzeti biztonsági felügyelete kérheti a másik Fél nemzeti biztonsági felügyeletétől biztonsági ellenőrzés lefolytatását a minősített adatok folyamatos védelmének biztosítása céljából a másik Fél országának területén működő, a minősített szerződéssel érintett létesítményben.

(4) Minden minősített szerződés vagy alvállalkozói szerződés részét képezi a projekt biztonsági utasítás, amely a szerződő minősített adatok védelmére vonatkozó kötelezettségeit és a minősített szerződés valamennyi elemének minősítési szintjével kapcsolatos rendelkezéseket határozza meg. A projekt biztonsági utasítás másolatát azon Fél nemzeti biztonsági felügyelete részére kell továbbítani, amelynek joghatósága alatt a minősített szerződés teljesítése történik.

(5) A szerződő minősített adatok védelmére vonatkozó kötelezettségei között legalább az alábbiaknak kell szerepelniük:
a) hozzáférés biztosítása a minősített adatokhoz a nemzeti jogszabályok és egyéb szabályok rendelkezéseivel, valamint jelen Egyezménnyel összhangban;
b) minősített adat továbbítása a jelen Egyezményben meghatározott módon;
c) tájékoztatás adása minden olyan változásról, amely a minősített adat vonatkozásában következett be;
d) a minősített szerződés hatálya alá tartozó minősített adatnak kizárólag a szerződés tárgya szerint meghatározott célokra történő felhasználása;
e) jelen Egyezménynek, a minősített adatok kezelésével kapcsolatos eljárásokra vonatkozó intézkedéseinek szigorú betartása;
f) a szerződő nemzeti biztonsági felügyeletének tájékoztatása a minősített adat biztonságának a minősített szerződés vonatkozásában bekövetkezett bárminemű megsértéséről;
g) a minősített szerződéssel kapcsolatos minősített adat harmadik fél részére történő átadása kizárólag az Átadó Fél előzetes, írásbeli hozzájárulásával.

(6) A minősített szerződésbe bevont alvállalkozónak a szerződőre vonatkozó biztonsági előírásoknak kell megfelelnie.

9. CIKK

A MINŐSÍTETT ADAT TOVÁBBÍTÁSA

(1) A minősített adat továbbítása az Átadó Fél nemzeti jogszabályainak és egyéb szabályainak rendelkezéseivel összhangban diplomáciai úton vagy a nemzeti biztonsági felügyeletek által írásban meghatározott egyéb módon történik. Az Átvevő Fél a „Titkos!" / TAJNO / SECRET vagy magasabb szintű minősített adat átvételének megtörténtét megerősíti. Minden más minősített adat átvételének megtörténtét csak arra irányuló kérelemre kell megerősíteni.

(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!" / VRLO TAJNO / TOP SECRET minősítésű adat fordítása vagy sokszorosítása kizárólag az Átadó Fél előzetes írásbeli hozzájárulásával lehetséges.

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

(5) Az Átadó Fél a minősített adat felhasználásának esetleges feltételhez kötésével kifejezetten megtilthatja a minősített adat megsemmisítését. A minősített adat megsemmisítésének megtiltása esetén a minősített adatot az Átadó Félnek vissza kell küldeni.

(6) Azt a minősített adatot, amelyre már nincs szükség, és amelynek megsemmisítése jelen cikk (4) és (5) bekezdése szerint nincs megtiltva, oly módon kell megsemmisíteni, hogy annak teljes vagy részleges helyreállítása lehetetlenné váljon.

(7) A minősített adatot olyan válsághelyzet esetén, amely lehetetlenné teszi annak védelmét, vagy ha annak az Átadó Félhez való visszajuttatása nem lehetséges, késedelem nélkül meg kell semmisíteni. A minősített adat megsemmisítéséről az Átvevő Fél nemzeti biztonsági felügyelete az Átadó Fél nemzeti biztonsági felügyeletét írásban, késedelem nélkül értesíti.

11. CIKK

LÁTOGATÁSOK

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

(2) A látogatást kezdeményező Fél nemzeti biztonsági felügyelete a tervezett látogatásról a fogadó Fél nemzeti biztonsági felügyeletének legalább húsz nappal a látogatás időpontja előtt megkeresést küld. 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 alábbi adatokat kell tartalmaznia:
a) a látogató vezetékneve és keresztneve, születési helye és ideje, állampolgársága, útlevelének vagy más személyazonosító igazolványának száma;
b) a látogató beosztásának és a látogató által képviselt jogi személy 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, beleértve a látogatással érintett legmagasabb minősítési szintű minősített adat minősítési szintjének megjelölését;
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;
h) minden egyéb adat, amelyről a nemzeti biztonsági felügyeletek megállapodtak.

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

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

(6) A Felek a nemzeti jogszabályaik és egyéb szabályaik rendelkezéseivel összhangban biztosítják a látogatók személyes adatainak védelmét.

12. CIKK

MINŐSÍTETT ADAT BIZTONSÁGÁNAK MEGSÉRTÉSE

(1) A nemzeti biztonsági felügyeletek késedelem nélkül írásban tájékoztatják egymást a jelen Egyezmény alapján keletkezett vagy kicserélt minősített adat biztonságának megsértéséről, vagy ha mindezek alapos gyanúja merül fel.

(2) Azon Fél nemzeti biztonsági felügyelete, ahol a minősített adat biztonságának megsértésére sor került, késedelem nélkül intézkedik a minősített adat megsértésének kivizsgálása iránt, és kezdeményezi a megfelelő eljárások lefolytatását a megsértés körülményeinek feltárása érdekében. A másik Fél nemzeti biztonsági felügyelete szükség esetén közreműködik a vizsgálatban és az eljárásokban.

(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 és az eljárások eredményéről.

(4) Ha a minősített adat biztonságának megsértése harmadik államban következik be, a nemzeti biztonsági felügyeletek késedelem nélkül meghatározzák a lehetséges károk minimalizálását célzó eljárásokat és intézkedéseket.

13. CIKK

KÖLTSÉGEK VISELÉSE

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

14. CIKK

ZÁRÓ RENDELKEZÉSEK

(1) Jelen 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.

(2) Jelen Egyezmény határozatlan időre jön létre. Bármelyik Fél jogosult jelen Egyezményt bármikor felmondani a másik Félnek diplomáciai úton küldött írásbeli értesítése útján. Felmondás esetén az Egyezmény a felmondásról szóló értesítés másik Fél általi kézhezvételétől számított hat hónap elteltével hatályát veszti.

(3) Jelen Egyezmény a Felek kölcsönös egyetértésével írásban bármikor módosítható. A módosítások hatályba lépésével kapcsolatban jelen cikk (1) bekezdésében foglaltak az irányadók.

(4) Az Egyezmény megszűnésétől függetlenül jelen Egyezmény alapján keletkezett vagy kicserélt valamennyi minősített adatot az Egyezményben meghatározott rendelkezések szerint kell védelemben részesíteni, mindaddig, amíg a Felek erről írásban eltérően nem döntenek.

(5) Jelen Egyezmény végrehajtásából vagy értelmezéséből fakadó vitákat a Felek egymás közötti egyeztetés vagy tárgyalás útján, nemzetközi bíróság vagy harmadik Fél igénybevétele nélkül rendezik.

Készült Budapesten, 2016. június 10-én, két eredeti példányban, magyar, horvát és angol nyelven, valamennyi szöveg egyaránt hiteles. Eltérő értelmezés esetén az angol nyelvű szöveg az irányadó.

Magyarország Kormánya részéről **a Horvát Köztársaság Kormánya részéről**

AGREEMENT

BETWEEN

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

The Government of Hungary and the Government of the Republic of Croatia (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 of Classified Information,

Wishing to ensure the protection of Classified Information exchanged between them or between the legal entities or individuals under their jurisdiction,

Mutually respecting national interests and security,

Have agreed as follows:

ARTICLE 1
OBJECTIVE AND APPLICABILITY OF THE AGREEMENT

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

2. This Agreement shall not affect the obligations of the Parties under any other bilateral or multilateral agreement, including any agreements governing exchange and mutual protection of Classified Information, except when this Agreement contains stricter regulations regarding the exchange or mutual protection of Classified Information.

ARTICLE 2
DEFINITIONS

For the purposes of this Agreement:

a) **"Classified Information"** means any information that, regardless of its form or nature, in accordance with the national laws and regulations of either Party, requires protection against Breach of Security and has been duly designated and marked appropriately;

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

c) "**Security Classification Level**" means a category which, in accordance with national laws and regulations, characterises the level of restriction of access to Classified Information and the minimum level of its protection;

d) **"Breach of Security**" means any act or 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 of Classified Information, or any other type of loss of its confidentiality, integrity or availability;

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

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

g) "**National Security Authority**" means the state authority responsible for the implementation and supervision of this Agreement;

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

i) "**Facility Security Clearance Certificate**" means the determination by the National Security 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;

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

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

l) **"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 Croatia:
Ured Vijeća za nacionalnu sigurnost (Office of the National Security Council).

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

3. The Parties shall inform each other through diplomatic channels of any subsequent changes of the National Security Authorities.

ARTICLE 4
SECURITY CLASSIFICATION LEVELS AND MARKINGS

1. Any Classified Information generated or exchanged under this Agreement shall be marked with the appropriate Security Classification Level in accordance with national laws and regulations of the Parties.

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

In Hungary	In the Republic of Croatia	Equivalent in English language
„Szigorúan titkos!”	VRLO TAJNO	TOP SECRET
„Titkos!”	TAJNO	SECRET
„Bizalmas!”	POVJERLJIVO	CONFIDENTIAL
„Korlátozott terjesztésű!”	OGRANIČENO	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, to whom an appropriate Personnel Security Clearance Certificate has been issued in accordance with the national laws and regulations and who have been briefed on their responsibilities for the protection of Classified Information.

ARTICLE 6
SECURITY PRINCIPLES

1. In accordance with their national laws and regulations, the Parties shall take all appropriate measures for the protection of Classified Information generated or exchanged under this Agreement.

2. 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 delay of any subsequent changes in the Security Classification Level or duration of classification.

3. 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 the same level of protection to Classified Information as afforded to its own Classified Information of equivalent Security Classification Level in accordance with Article 4 of this Agreement;
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 use conditions of the Originating Party.

ARTICLE 7
SECURITY COOPERATION

1. In order to maintain compatible standards of security, the National Security Authorities shall, on request, inform each other of their national laws and regulations concerning the protection of Classified Information and the practices stemming from their implementation. The National Security Authorities shall inform each other of any subsequent changes in their national laws and regulations concerning Classified Information.

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 Clearance Certificates and the Facility Security Clearance Certificates issued by 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 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 the proposed Contractors as well as individuals participating in pre-contractual negotiations or in the implementation of Classified Contracts at the level „Bizalmas!" / POVJERLJIVO / CONFIDENTIAL or above have an appropriate Personnel Security Clearance Certificate or Facility Security Clearance Certificate.

2. If the proposed Contractor does not hold an appropriate security clearance certificate, the National Security Authority of the Originating Party may request the National Security Authority of the Recipient Party to issue the appropriate security clearance certificate.

3. The National Security Authority of one Party may request from the National Security Authority of the other Party that a security inspection is carried out to ensure continuing protection of Classified Information at a facility located on the territory of the other Party which has been involved in the Classified Contract.

4. Each Classified Contract or sub-contract shall contain Project Security Instructions on the security requirements, including the Contractor's obligations to protect Classified Information, 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.

5. The Contractor's obligations to protect Classified Information shall include, at least, the following:
a) granting access to Classified Information in accordance with the national laws and regulations and this Agreement;

b) transferring and transmitting Classified Information by the means specified in this Agreement;
c) communicating any changes that may arise in respect of the Classified Information;
d) using the Classified Information under the Classified Contract only for the purposes related to the subject of the contract;
e) adhering strictly to the provisions of this Agreement related to the procedures for handling Classified Information;
f) notifying the Contractor's National Security Authority of any Breach of Security related to the Classified Contract;
g) releasing the Classified Information related to the Classified Contract to any Third Party only upon prior written consent of the Originating Party.

6. Sub-contractors engaged in Classified Contracts shall comply with the security instructions which apply to the Contractors.

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. The Recipient Party shall confirm the receipt of Classified Information at the levels „Titkos!" / TAJNO / SECRET and above. The receipt of other Classified Information shall be confirmed on request.

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!" / VRLO TAJNO / 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!" / VRLO TAJNO / TOP SECRET shall not be destroyed and shall be returned to the Originating Party.

5. The Originating Party may, by adding a use condition, expressly prohibit the destruction of Classified Information. If the destruction of Classified Information is prohibited, it shall be returned to the Originating Party.

6. Classified Information the destruction of which is not prohibited in accordance with paragraphs 4 and 5 of this Article and which is no longer needed shall be destroyed in a way which prevents its reconstruction in whole or in part.

7. 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 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 without delay.

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 coordination between the National Security Authorities.

3. The request for visit shall contain:

a) visitor's first name and last 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;

h) any other data, agreed upon by the National Security Authorities.

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 exchanged under this Agreement.

6. Each Party shall guarantee the protection of the personal data of the visitors in accordance with its national laws and regulations.

ARTICLE 12
BREACH OF SECURITY

1. The National Security Authorities shall, without delay, inform each other in writing of any Breach of Security of Classified Information generated or exchanged under this Agreement or profound suspicion thereof.

2. The National Security Authority of the Party where the Breach of Security has occurred shall inspect the incident and initiate other appropriate proceedings to determine the circumstances of the breach without delay. The National Security Authority of the other Party shall, if required, cooperate in the inspection and the proceedings.

3. In any case, the National Security Authority of the Recipient Party shall inform the National Security Authority of the Originating Party in writing about the circumstances of the Breach of Security, the extent of the damage, the measures applied for its mitigation and the outcome of the inspection and the proceedings.

4. When the Breach of Security has occurred in a third state, the National Security Authorities shall agree upon the actions and measures to be taken without delay to minimize the possible damage.

ARTICLE 13
EXPENSES

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

ARTICLE 14
FINAL PROVISIONS

1. This Agreement shall enter into force on the first day of the second month following the date of receipt of the last written notification by which the Parties have informed each other, through diplomatic channels, that their internal legal requirements necessary for its entry into force have been fulfilled.

2. This Agreement is concluded for an indefinite period of time. Each Party may terminate this Agreement at any time by written notification to the other Party, through diplomatic channels. In

such a case, the Agreement shall terminate six months from the date on which the termination notice has been received by the other Party.

3. This Agreement may be amended at any time by mutual written consent of the Parties. Such amendments shall enter into force in accordance with paragraph 1 of this Article.

4. Notwithstanding the termination of this Agreement, all Classified Information generated or exchanged under this Agreement shall continue to be protected in accordance with the provisions of this Agreement, unless the Parties agree otherwise in writing.

5. Any dispute regarding the interpretation or implementation of this Agreement shall be settled by consultations and negotiations between the Parties and shall not be referred to any international tribunal or Third Party for settlement.

Done at Budapest on 10th June 2016 in two originals, each in the Hungarian, Croatian and English languages, all texts being equally authentic. In case of any divergences in interpretation, the English text shall prevail.

For the Government of Hungary	**For the Goverment of the Republic of Croatia”**

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 Horvát 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 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 15-én Spanyolországgal, 2016. október 6-án Montenegróval.

2016. június 10-én, Budapesten sor került *a Magyarország Kormánya és a Horvát Köztársaság Kormánya között a minősített adatok cseréjéről és kölcsönös védelméről szóló egyezmény* (a továbbiakban: Egyezmény) aláírására, amelyre *a Magyarország Kormánya és a Horvát Köztársaság Kormánya között a minősített adatok cseréjéről és kölcsönös védelméről szóló egyezmény szövegének végleges megállapítására adott felhatalmazásról szóló 1517/2015. (VII. 23.) 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.