MAGYARORSZÁG KORMÁNYA

T/2919. számú

törvényjavaslat

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

Előadó: **Dr. Pintér Sándor**
belügyminiszter

Budapest, 2015. január

2015. évi … törvény

Magyarország Kormánya és a Macedón 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 Macedón 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, macedón és angol nyelvű szövege a következő:

”

EGYEZMÉNY

MAGYARORSZÁG KORMÁNYA ÉS A MACEDÓN KÖZTÁRSASÁG KORMÁNYA

KÖZÖTT

A MINŐSÍTETT ADATOK CSERÉJÉRŐL ÉS KÖLCSÖNÖS VÉDELMÉRŐL

Magyarország Kormánya és a Macedón Köztársaság Kormánya (a továbbiakban együtt: Felek),

Elismerve a Felek közötti kölcsönös együttműködés jelentőségét a béke stabilizálása, a nemzetközi biztonság és kölcsönös bizalom megteremtése érdekében,

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

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

Kívánatosnak tartva, hogy a közöttük, illetve a joghatóságuk alá tartozó jogi személyek és természetes személyek között 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 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 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) A „**Minősített Adat**” megjelenési formájától vagy természetétől függetlenül, minden olyan adat, amelyet bármelyik Fél nemzeti jogszabályai szerint védelemben kell részesíteni a minősített adat biztonságának megsértésével szemben, s amelyet ennek megfelelően minősítettek;

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

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

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

e) A „**Szerződő**” olyan természetes személy vagy jogi személy, amely a nemzeti jogszabályokkal összhangban jogképességgel rendelkezik minősített szerződések megkötésére;

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

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

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

i) A „**Nemzeti Biztonsági Felügyelet**” az érintett Fél azon hatóságát jelenti, amely a minősített adatok védelméért, valamint jelen egyezmény alkalmazásáért és felügyeletéért felelős.

3. Cikk

Nemzeti Biztonsági Felügyeletek

1. A Felek Nemzeti Biztonsági Felügyeletei a következők:

Magyarországon:

Nemzeti Biztonsági Felügyelet

A Macedón Köztársaságban:

Minősített Információbiztonsági Igazgatóság (Дирекција за безбедност на класифицирани информации)

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

4. Cikk

Minősítési szintek megfeleltetése

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

Magyarországon	**A Macedón Köztársaságban**	**Angol nyelvű megfelelőjük**
„Szigorúan titkos!”	ДРЖАВНА ТАЈНА	TOP SECRET
„Titkos!”	СТРОГО ДОВЕРЛИВО	SECRET
„Bizalmas!”	ДОВЕРЛИВО	CONFIDENTIAL
„Korlátozott terjesztésű!”	ИНТЕРНО	RESTRICTED

5. Cikk

Minősített adathoz való hozzáférés

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

6. Cikk

Biztonsági alapelvek

1. Az Átadó Fél:

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

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

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

2. Az Átvevő Fél:

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

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

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

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

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

7. Cikk

Biztonsági együttműködés

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

2. Megkeresés esetén a Nemzeti Biztonsági Felügyeletek, összhangban a nemzeti jogszabályaik rendelkezéseivel, kölcsönösen segítséget nyújtanak egymásnak a személyi biztonsági tanúsítványokkal és a telephely biztonsági tanúsítványokkal kapcsolatos eljárások során.

3. Megkeresés esetén a Felek nemzeti jogszabályaik rendelkezéseivel összhangban elismerik a másik Fél által kibocsátott személyi biztonsági tanúsítványokat és telephely biztonsági tanúsítványokat. Mindezek során a jelen Egyezmény 4. Cikkében foglaltakat megfelelően kell alkalmazni.

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 során megvalósuló együttműködés angol nyelven történik.

8. Cikk

Minősített szerződések

1. A minősített szerződéseket a Felek saját nemzeti jogszabályai alapján kell megkötni és teljesíteni. A Nemzeti Biztonsági Felügyeletek megkeresésre kötelesek megerősíteni, hogy az ajánlattevő és az előzetes szerződési tárgyalásokban vagy a minősített szerződések teljesítésében részt vevő természetes személyek rendelkeznek megfelelő személyi biztonsági tanúsítvánnyal vagy telephely biztonsági tanúsítvánnyal.

2. A Nemzeti Biztonsági Felügyeletek kérelmezhetik, hogy a másik Fél biztonsági ellenőrzést folytasson le a területén működő létesítményben a minősített adat folyamatos védelmének biztosítása céljából.

3. A minősített szerződések részét képezi a projekt biztonsági utasítás, amely a biztonsági követelményeket és a szerződés egyes elemeinek minősítésével kapcsolatos rendelkezéseket határozza meg. A projekt biztonsági utasítás másolatát azon Fél Nemzeti Biztonsági Felügyelete részére kell továbbítani, amelynek joghatósága alatt a minősített szerződés végrehajtása történik.

9. Cikk

A minősített adat továbbítása

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

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

10. Cikk

A minősített adat sokszorosítása, fordítása és megsemmisítése

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

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

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

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

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

11. Cikk

Látogatások

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

2. A látogató Fél Nemzeti Biztonsági Felügyelete köteles a fogadó Fél Nemzeti Biztonsági Felügyeletét legalább 20 nappal a látogatás időpontja előtt tájékoztatni a tervezett látogatásról. Sürgős esetben, a Nemzeti Biztonsági Felügyeletek előzetes egyeztetését követően a látogatásra vonatkozó megkeresés a látogatás kezdetéhez közelebbi időpontban is benyújtható.

3. A látogatásra vonatkozó megkeresésnek az alábbiakat kell tartalmaznia:

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

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

c) a látogató személyi biztonsági tanúsítványának szintje és érvényességi ideje;

d) a látogatás időpontja és időtartama, visszatérő látogatások esetén az egyes látogatások összesített időtartama;

e) a látogatás célja, valamint a megismerendő legmagasabb minősítési szintű minősített adat minősítési szintjének megjelölése;

f) a meglátogatandó létesítmény neve és címe, valamint a kapcsolattartójának neve, telefonszáma, faxszáma, e-mail címe;

g) dátum, aláírás és a Nemzeti Biztonsági Felügyelet hivatalos pecsétjének lenyomata.

4. A Nemzeti Biztonsági Felügyeletek közösen meghatározhatják a visszatérő látogatásra jogosult személyek listáját. A visszatérő látogatások további részleteit a Nemzeti Biztonsági Felügyeletek közösen állapítják meg.

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

12. Cikk

Eljárás a minősített adat biztonságának megsértése esetén

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

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

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

13. Cikk

Költségek viselése

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

14. Cikk

Záró rendelkezések

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

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

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

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

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

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

Készült Szkopjéban, 2014. július 3-án, két eredeti példányban, magyar, macedón és angol nyelven, valamennyi szöveg egyaránt hiteles. Eltérés esetén az angol nyelvű szöveg az irányadó.

Magyarország Kormánya részéről	**A Macedón Köztársaság Kormánya részéről**

СПОГОДБА МЕЃУ

ВЛАДАТА НА УНГАРИЈА

И

ВЛАДАТА НА РЕПУБЛИКА МАКЕДОНИЈА

ЗА РАЗМЕНА И ЗАЕМНА ЗАШТИТА

НА КЛАСИФИЦИРАНИ ИНФОРМАЦИИ

Владата на Унгарија и Владата на Република Македонија (во натамошниот текст наречени „Страни“),

Признавајќи ја важноста на заемната соработка меѓу Страните за стабилизација на мирот, меѓународната безбедност и заемната доверба,

Согледувајќи дека добрата соработка може да бара и размена на класифицирани информации меѓу Страните,

Признавајќи дека можат да осигураат подеднаква заштита за класифицираните информации,

Сакајќи да обезбедат заштита на класифицираните информации што се разменети меѓу нив или меѓу правните лица или физичките лица под нивна надлежност,

Со заемно почитување на националните интереси и безбедноста, се согласија за следното:

ЧЛЕН 1

ЦЕЛ И ПРИМЕНА НА СПОГОДБАТА

1. Целта на оваа спогодба е да се обезбеди заштита на класифицираните информации што се разменети или создадени во текот на соработката меѓу Страните или меѓу правните лица или физичките лица што се под нивна надлежност.

2. Оваа спогодба нема да влијае на обврската на Страните што произлегува од некој друг билатерален или мултилатерален договор, вклучувајќи и договори за размена и заемна заштита на класифицирани информации.

ЧЛЕН 2

ДЕФИНИЦИИ

За целите на оваа спогодба:

а) **„Класифицирана информација”** е која било информација којашто, без оглед на нејзината форма или природа, во согласност со националните закони и регулативи на секоја од Страните, треба да се заштити од нарушување на безбедноста и којашто е соодветн означена;

б) **„Нарушување на безбедноста“** е чин или пропуст којшто е спротивен на оваа спогодба или на националните закони и регулативи на Страните и којшто може да резултира со неовластено откривање, губење, уништување, злоупотреба или некој друг вид на загрозување на класифицираните информации;

в) **„Потребно е да знае“** е принцип според којшто пристап до одредена класифицирана информација може да се даде само на лице коешто има утврдена потреба за пристап до таа класифицирана информација во врска со неговите/нејзините службени должности или заради извршување на специфична задача;

г) **„Класифициран договор”** е договор којшто вклучува или за којшто е потребен пристап до класифицирани информации.

д) **„Контрактор“** е физичко или правно лице коешто поседува правна способност да склучува класифицирани договори во согласност со националните закони и регулативи;

ѓ) **„Страна-создавач”** е Страната вклучувајќи ги и правните лица или физичките лица под нејзина надлежност, којашто отстапува на користење класифицирани информации;

е) **„Страна-примач”** е Страната вклучувајќи ги и правните лица или физичките лица под нејзина надлежност, којашто прима класифицирани информации;

ж) **„Трета страна”** е која било држава вклучувајќи ги и правните лица или физичките

лица под нејзина надлежност или меѓународна организација коишто не се страна на оваа спогодба;

з) **„Национален безбедносен орган“** е органот на соодносната страна којшто е одговорен за заштитата на класифицираните информации, како и за спроведувањето и надзорот над оваа спогодба.

ЧЛЕН 3

НАЦИОНАЛНИ БЕЗБЕДНОСНИ ОРГАНИ

1. Националните безбедносни органи на Страните се:

Во Унгарија:

Nemzeti Biztonsági Felügyelet (National Security Authority)

Во Република Македонија:

Дирекција за безбедност на класифицирани информации (Directorate for Security of Classified Information)

2. Националните безбедносни органи заемно се известуваат за деталите за официјален контакт и заемно се информираат за секоја нивна последователна измена.

ЧЛЕН 4

СТЕПЕНИ НА БЕЗБЕДНОСНА КЛАСИФИКАЦИЈА И ОБЕЛЕЖУВАЊЕ

Еквивалентни национални степени за безбедносна класификација и обележување се:

Во Унгарија	**Во Република Македонија**	**Еквивалент на англиски јазик**
„Szigorúan titkos!”	ДРЖАВНА ТАЈНА	TOP SECRET
„Titkos!”	СТРОГО ДОВЕРЛИВО	SECRET
„Bizalmas!”	ДОВЕРЛИВО	CONFIDENTIAL
„Korlátozott terjesztésű!”	ИНТЕРНО	RESTRICTED

ЧЛЕН 5

ПРИСТАП ДО КЛАСИФИЦИРАНИ ИНФОРМАЦИИ

Пристапот до класифицираните информации во согласност со оваа спогодба е ограничен само на физичките лица според принципот „потребно е да знае“ и коишто се соодветно овластени за тоа во согласност со националните закони и регулативи на соодносната Страна.

ЧЛЕН 6

БЕЗБЕДНОСНИ ПРИНЦИПИ

1. Страната-создавач треба да:

а) осигура класифицираната информација да биде обележана со соодветни ознаки за безбедносна класификација во согласност со нејзините националните закони и регулативи;

б) ја информира Страната-примач за условите за користење на класифицираната информација;

в) ја информира Страната-примач без непотребно одлагање за последователните промени во степенот на безбедносната класификација.

2. Страната-примач треба да:

а) осигура класифицираната информација да биде обележана со еквивалентна ознака за безбедносна класификација во согласност со член 4 од оваа спогодба;

б) го пружи истиот степен на заштита на класифицираната информација како и за сопствените класифицирани информации со еквивалентен степен на безбедносна класификација;

в) осигура дека класифицираната информација не е декласифицирана ниту пак дека е променет степенот на нејзината безбедносна класификација без претходна писмена согласност на Страната-создавач;

г) осигура класифицираната информација да не биде отстапена на користење на Трета страна без претходна писмена согласност на Страната-создавач;

д) ја користи класифицираната информација само за целта за којашто и е отстапена и под условите за користење класифицирани информации на Страната-создавач.

ЧЛЕН 7

БЕЗБЕДНОСНА СОРАБОТКА

1. Со цел да одржат споредливи стандарди за безбедност, Националните безбедносни органи, на барање, заемно се информираат за нивните национални закони и регулативи во врска со заштитата на класифицираните информации и за практиките што произлегуваат од нивното спроведување.

2. На барање, Националните безбедносни органи, во согласност со нивните национални закони и регулативи, заемно си помагаат во текот на процедурите сврзани со безбедносен сертификат на физички лица и со безбедносен сертификат за правни лица.

3. На барање, Страните во согласност со нивните национални закони и регулативи ги признаваат безбедносните сертификати за физички лица и безбедносните сертификати за правни лица издадени од другата Страна. Членот 4 од оваа спогодба се применува соодветно.

4. Националните безбедносни органи без одлагање заемно се известуваат за сите промени во признаените безбедносни сертификати за физички лица и во признаените безбедносни сертификати за правни лица, особено во случај на нивно повлекување.

5. Соработката во рамките на оваа спогодба се изведува на англиски јазик.

ЧЛЕН 8

КЛАСИФИЦИРАНИ ДОГОВОРИ

1. Класифицирани договори се склучуваат и спроведуваат во согласност со националните закони и регулативи на секоја од Страните. На барање, Националните безбедносни органи потврдуваат дека предложените контрактори и физичките лица коишто учествуваат во пред-договорните преговори или во спроведувањето на класифицираните договори имаат соодветен безбедносен сертификат за физички лица или безбедносен сертификат за правни лица.

2. Националниот безбедносен орган може да побара од наспроти поставениот орган да спроведе безбедносна инспекција на правното лице што се наоѓа на територијата на другата Страна со цел да се осигура континуирана заштита на класифицираните информации.

3. Класифицираните договори треба да содржат инструкции за безбедност на проектот, безбедносните потреби и за степенот на безбедносна класификација на секој елемент од класифицираниот договор. Копија од инструкциите за безбедност на проектот се доставува до Националниот безбедносен орган на Страната под чија надлежност ќе се спроведува класифицираниот договор.

ЧЛЕН 9

ПРЕНОС И ИСПРАЌАЊЕ НА КЛАСИФИЦИРАНИ ИНФОРМАЦИИ

1. Класифицираните информации се пренесуваат во согласност со националните закони и регулативи на Страната-создавач преку дипломатски пат или на друг начин договорен писмено меѓу Националните безбедносни органи.

2. Страните можат да испраќаат класифицирани информации преку електронски средства во согласност со безбедносните процедури одобрени писмено од страна на Националните безбедносни органи.

ЧЛЕН 10

УМНОЖУВАЊЕ, ПРЕВОД И УНИШТУВАЊЕ НА КЛАСИФИЦИРАНИ ИНФОРМАЦИИ

1. Копиите и преводите на класифицираните информации отстапени на користење во согласност со оваа спогодба носат соодветни ознаки за безбедносна класификација и се заштитуваат како и оригиналите. Бројот на копии се ограничува на број потребен за официјални цели.

2. На преводите на класифицираните информации отстапени на користење во согласност со оваа спогодба стои соодветна забелешка на јазикот на којшто се преведени дека содржат класифицирани информации на Страната-создавач.

3. Класифицираните информации отстапени на користење во согласност со оваа спогодба со ознака „Szigorúan titkos!”/ ДРЖАВНА ТАЈНА / TOP SECRET се преведуваат или умножуваат само по претходна писмена согласност од Страната-создавач.

4. Класифицираните информации отстапени на користење во согласност со оваа спогодба со ознака „Szigorúan titkos!”/ ДРЖАВНА ТАЈНА / TOP SECRET не се уништуваат и треба да се вратат на Страната-создавач.

5. Во случај на кризна ситуација во којашто е невозможно да се заштитат или да се вратат класифицираните информации на Страната-создавач се уништуваат без непотребно одлагање. Националниот безбедносен орган на Страната-примач писмено го известува Националниот безбедносен орган на Страната-создавач за уништувањето на класифицираните информации.

ЧЛЕН 11

ПОСЕТИ

1. Посетите за коишто е потребен пристап до класифицирани информации се предмет на претходно писмено одобрение од страна на Националниот безбедносен орган на сообоснатa Страна.

2. Националниот безбедносен орган на Страната посетител го известува Националниот безбедносен орган на Страната домаќин за планираната посета преку барање за посета најмалку дваесет дена пред посетата. Во итни случаи, барањето за посета може да се достави и за пократко време, по претходна координација меѓу Националните безбедносни органи.

3. Барањето за посета содржи:

а) име на посетителот, датум и место на раѓање, државјанство и број на пасош/лична карта;

б) позиција на посетителот и спецификација на правното лице што го претставува;

в) статус на безбедносниот сертификат на посетителот и неговата валидност;

г) датум и времетраење на посетата, а во случај на повторливи посети вкупниот временски период на посетите;

д) целта на посетата вклучително со највисокиот степен на безбедносна класификација на вклучените класифицираните информации;

ѓ) назив и адреса на објектот што се посетува, како и име, број на телефон/факс, е-маил адреса на лицето за контакт;

е) датум, потпис и отпечаток на официјалниот печат на Националниот безбедносен орган.

4. Националните безбедносни органи можат да договорат листа на посетители со право на повторливи посети. Националните безбедносни органи ги договараат понатамошните детали за повторливите посети.

5. Класифицираните информации што ги добива посетителот се сметаат за класифицирани информации примени во согласност со оваа спогодба.

ЧЛЕН 12

НАРУШУВАЊЕ НА БЕЗБЕДНОСТА

1. Националните безбедносни органи без непотребно одлагање писмено се информираат за нарушувањето на безбедноста или за постоењето сомнеж за такво нарушување на безбедноста.

2. Националниот безбедносен орган на Страната каде што настанало нарушувањето на безбедноста презема мерки, без непотребно одлагање и во согласност со националните закони и регулативи, за истражување на инцидентот. Националниот безбедносен орган на другата Страна, доколку е потребно, соработува во истражувањето.

3. Во секој случај, Националниот безбедносен орган на Страната-примач писмено го известува Националниот безбедносен орган на Страната-создавач за околностите на нарушувањето на безбедноста, за опфатот на штетата, за мерките преземени за нејзино ублажување и за резултатот од истражувањето.

ЧЛЕН 13

ТРОШОЦИ

Секоја Страна ги сноси своите трошоци настанати во текот на спроведувањето на оваа спогодба.

ЧЛЕН 14

ЗАВРШНИ ОДРЕДБИ

1. Оваа спогодба се склучува на неопределено време. Оваа спогодба влегува во сила на првиот ден од вториот месец по добивање на последното известување со кое Страните заемно се известуваат преку дипломатски пат дека националните правни барања за влегување во сила на оваа спогодба се исполнети.

2. Оваа спогодба може да се менува врз основа на заемна писмена согласност на Страните. Измените влегуваат во сила во согласност со одредбите од став 1 од овој член.

3. Секоја од Страните може да ја откаже оваа спогодба со доставување писмено известување во кое било време. Во тој случај, важноста на оваа спогодба истекува после шест месеци од денот на којшто другата Страна го примила писменото известување за откажувањето на спогодбата.

4. Без оглед на откажувањето на оваа спогодба, сите класифицирани информации разменети или создадени врз основа на оваа спогодба се заштитуваат во согласност со одредбите на оваа спогодба сè додека Страната-создавач писмено не ја ослободи Страната-примач од таквата обврска.

5. Сите спорови во врска со толкувањето или спроведувањето на оваа спогодба ќе се решаваат во консултации и преговори меѓу Страните без учество на трета страна.

За потврда на ова, долупотпишаните, соодветно овластени за оваа цел, ја потпишаа оваа спогодба.

Потпишана во Скопје на 3јули 2014 година во два оригинални примерока на унгарски, на македонски и на англиски јазик, пришто сите текстови се еднакво веродостојни. Во случај на разлики во толкувањето, ќе преовлада текстот на англиски јазик.

За Владата на	**За Владата на**
Унгарија	**Република Македонија**

AGREEMENT

BETWEEN THE GOVERNMENT OF HUNGARY AND THE GOVERNMENT OF THE REPUBLIC OF MACEDONIA

ON THE EXCHANGE AND MUTUAL PROTECTION OF CLASSIFIED INFORMATION

The Government of Hungary and the Government of the Republic of Macedonia (hereinafter referred to as the “Parties”),

Recognising the importance of mutual cooperation between the Parties for the stabilization of peace, international security and mutual confidence

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 or 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 or 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 has been duly designated;

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

c) **"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;

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

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

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

i) "**National Security Authority**" means the authority of the respective Party responsible for the protection of Classified Information as well as for the implementation and supervision of this Agreement.

ARTICLE 3

NATIONAL SECURITY AUTHORITIES

1. The National Security Authorities of the Parties are:

In Hungary:

Nemzeti Biztonsági Felügyelet (National Security Authority)

In the Republic of Macedonia:

Дирекција за безбедност на класифицирани информации (Directorate for Security of Classified Information)

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

ARTICLE 4

SECURITY CLASSIFICATION LEVELS AND MARKINGS

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

In Hungary	**In the Republic of Macedonia**	**Equivalent in English language**
„Szigorúan titkos!”	ДРЖАВНА ТАЈНА	TOP SECRET
„Titkos!”	СТРОГО ДОВЕРЛИВО	SECRET
„Bizalmas!”	ДОВЕРЛИВО	CONFIDENTIAL
„Korlátozott terjesztésű!”	ИНТЕРНО	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

SECURITY PRINCIPLES

1. The Originating Party shall:

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

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

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

2. The Recipient Party shall:

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

b) afford 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 under the conditions for use of Classified Information 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. 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 facility security clearance certificates issued by the other Party. Article 4 of this Agreement shall apply accordingly.

4. The National Security Authorities shall without undue delay 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 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 certificate or facility security clearance certificate.

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

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

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

ARTICLE 11

VISITS

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

2. The National Security Authority of the visiting Party shall notify the National Security Authority of the host Party about the planned visit through a request for visit at least twenty days before the visit takes place. In urgent cases, the request for visit may be submitted at a shorter notice, subject to prior co-ordination between the National Security Authorities.

3. The request for visit shall contain:

a) visitor's name, date and place of birth, nationality and passport/ID card number;

b) position of the visitor and specification of the legal entity represented;

c) visitor's personnel security clearance certificate status 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 make provisions, in accordance with the national laws and regulations, for the investigation of the incident without undue delay. 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.

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 Skopje on 3th July 2014 in two originals, in Hungarian, Macedonian 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 Macedonia”**

4. §

(1) Ez a törvény – a (2) bekezdésben meghatározott kivétellel – a kihirdetését követő napon lép hatályba.

(2) A 2. § és 3. § az Egyezmény 14. Cikk 1. pontjában meghatározott időpontban lép hatályba.

(3) Az Egyezmény, illetve a 2. § és 3. § hatálybalépésének naptári napját a külpolitikáért felelős miniszter annak ismertté válását követően a Magyar Közlönyben haladéktalanul közzétett közleményével állapítja meg.

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

INDOKOLÁS A MAGYARORSZÁG KORMÁNYA ÉS A MACEDÓN 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 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, macedón 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 kihirdetését követő napon lép hatályba. Az Egyezmény 14. Cikk 1. pontja szerinti hatálybalépés 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.