MAGYARORSZÁG KORMÁNYA

T/17299. számú

törvényjavaslat

a Magyarország Kormánya és a Ciprusi 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 Ciprusi 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 Ciprusi 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 CIPRUSI KÖZTÁRSASÁG KORMÁNYA KÖZÖTT
A MINŐSÍTETT ADATOK CSERÉJÉRŐL ÉS KÖLCSÖNÖS VÉDELMÉRŐL

Magyarország Kormánya és a Ciprusi Köztársaság Kormánya (a továbbiakban együtt: Szerződő Felek)

Elismerve a kölcsönös együttműködés fontos szerepét,

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

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

Tiszteletben tartva a Szerződő Felek minősített adatok védelmére vonatkozó közös érdekeit, nemzeti jogszabályaikkal összhangban,

Az alábbiakban állapodtak meg:

1. Cikk

Az Egyezmény tárgya

1. Jelen Egyezmény célja, hogy kölcsönös védelmet biztosítson az egyik Szerződő Fél által minősített és a másik Szerződő Fél részére továbbított vagy a Szerződő Felek, valamint

joghatóságuk alá tartozó jogi személyek vagy természetes személyek közötti együttműködés során keletkezett valamennyi minősített adat számára.

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

2. Cikk

Fogalommeghatározások

Jelen Egyezmény alkalmazásában:

a) A **„Minősített adat biztonságának megsértése”** jelen Egyezménnyel vagy a Szerződő Felek nemzeti jogszabályaival ellentétes olyan tevékenység vagy mulasztás, amelynek következtében a minősített adat jogosulatlan nyilvánosságra hozatala, elvesztése, megsemmisülése, jogosulatlan felhasználása, vagy egyéb módon történő megsértése következik be.

b) A „**Minősített Adat**” megjelenési formájától, természetétől függetlenül minden olyan adat, amelyet bármelyik Szerződő Fél nemzeti jogszabályai szerint védelemben kell részesíteni biztonságának megsértésével szemben, s amely ennek megfelelő minősítést kapott.

c) A „**Minősített Szerződés**” olyan szerződést jelent, amely minősített adatot tartalmaz vagy amely alapján minősített adathoz való hozzáférés szükséges.

d) A „**Szerződő**” olyan természetes személy vagy jogi személy, aki a nemzeti jogszabályokkal összhangban jogképességgel rendelkezik minősített szerződések megkötésére.

e) „**Nemzeti Biztonsági Felügyelet**” a Szerződő Felek azon hatóságait jelenti, amelyek a nemzeti jogszabályokkal összhangban jelen Egyezmény végrehajtásáért és felügyeletéért felelősek. Ezen hatóságok jelen Egyezmény 3. Cikk 1. bekezdésében vannak nevesítve.

f) A „**Szükséges Ismeret elve”** azt a követelményt jelenti, amely alapján a minősített adathoz történő hozzáférés csak olyan személy részére biztosítható, akinek a hozzáférés hivatali kötelezettsége teljesítéséhez vagy egyéb speciális feladata ellátásához szükséges.

g) „**Átadó Fél**” azt a Szerződő Felet, valamint joghatósága alá tartozó természetes vagy jogi személyeket jelenti, amelyek létrehozták a minősített adatot.

h) „**Átvevő Fél**” azt a Szerződő Felet, valamint joghatósága alá tartozó természetes vagy jogi személyeket jelenti, amelyek részére az Átadó Fél minősített adatot továbbít.

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

3. Cikk

A Nemzeti Biztonsági Felügyeletek

1. A Szerződő Felek jelen Egyezmény végrehajtásáért és felügyeletéért felelős, Nemzeti Biztonsági Felügyeletei a következők:

Magyarországon:

Nemzeti Biztonsági Felügyelet

A Ciprusi Köztársaságban:

Εθνική Αρχή ΑσφαλείαςΥπουργείο Αμυνας της Κυπριακής Δημοκρατίας/

Nemzeti Biztonsági Felügyelet, a Ciprusi Köztársaság Védelmi Minisztériuma

2. A Nemzeti Biztonsági Felügyeletek kötelesek egymást diplomáciai úton tájékoztatni hivatalos elérhetőségi adataikról, és az ezekben bekövetkezett valamennyi változásról.

3. Megkeresés esetén a Nemzeti Biztonsági Felügyeletek kötelesek egymást tájékoztatni más, hatáskörrel rendelkező hatóságaikról is.

4. A Nemzeti Biztonsági Felügyeletek kötelesek egymást tájékoztatni a minősített adatokkal kapcsolatos nemzeti jogszabályaikról és az ezekkel kapcsolatos valamennyi lényeges változásról valamint megkeresés esetén tájékoztatják egymást a minősített adatok védelmével kapcsolatos biztonsági előírásaikról, eljárásaikról és mindezek gyakorlati alkalmazásáról.

4. Cikk

Minősítési szintek megfeleltetése

A Szerződő Felek megállapodnak abban, hogy az alábbi nemzeti minősítési szintek egymással megfeleltethetők, és összhangban állnak a nemzeti jogszabályaikkal:

Magyarországon	**A Ciprusi Köztársaságban**	**Angol nyelvű megfelelőjük**
„Szigorúan titkos!”	ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ	TOP SECRET
„Titkos!”	ΑΠΟΡΡΗΤΟ	SECRET
„Bizalmas!”	ΕΜΠΙΣΤΕΥΤΙΚΟ	CONFIDENTIAL
„Korlátozott terjesztésű!”	ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ	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 az adott Szerződő Fél nemzeti jogszabályaival összhangban felhatalmazást kaptak az adott minősítési szintű minősített adathoz történő hozzáférésre.

6. Cikk

Biztonsági alapelvek

1. Szerződő Felek nemzeti jogszabályaikkal összhangban kötelesek megtenni valamennyi intézkedést a jelen Egyezmény alapján kicserélt vagy keletkezett minősített adat védelme érdekében.

2. 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 írásban tájékoztatni az Átvevő Felet az átadott minősített adat minősítésében bekövetkezett változásokról.

3. 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 átvett minősített adat minősítését az Átadó Fél előzetes írásbeli hozzájárulása nélkül nem szünteti meg, illetve minősítési szintjét nem változtatja meg;
d) köteles biztosítani, hogy az Átadó Fél előzetes írásbeli hozzájárulása nélkül az átvett minősített adatot Harmadik Fél részére nem adja át;
e) a minősített adatot kizárólag az átadás során megjelölt célra használhatja fel, betartva az Átadó Fél által meghatározott kezelési előírásokat.

7. Cikk

Biztonsági együttműködés

1. 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.

2. Jelen Egyezmény alapján a Szerződő Felek megkeresés esetén nemzeti jogszabályaik rendelkezéseivel összhangban elismerik a másik Szerződő Fél által kibocsátott személyi biztonsági tanúsítványokat és telephely biztonsági tanúsítványokat.

3. A Nemzeti Biztonsági Felügyeletek kötelesek haladéktalanul értesíteni egymást az elismert személyi biztonsági tanúsítványokkal és a telephely biztonsági tanúsítványokkal kapcsolatos valamennyi változásról, különösen azok visszavonásáról vagy leminősítéséről.

4. Jelen Egyezmény végrehajtása során a Nemzeti Biztonsági Felügyeletek az angol nyelvet használják.

8. Cikk

Minősített szerződések

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

2. A Nemzeti Biztonsági Felügyeletek kérelmezhetik, hogy a másik Szerződő Fél biztonsági ellenőrzést folytasson le a területén működő létesítményben, biztosítván a minősített adat védelmét szolgáló intézkedések folyamatos alkalmazását.

3. A szerződő a nemzeti jogszabályok alapján tájékoztatást ad valamennyi lehetséges alvállalkozóról annak a Nemzeti Biztonsági Felügyeletnek, amelynek területén a minősített szerződés teljesítése történik.

4. A minősített szerződések részét képezi a projekt biztonsági utasítás, amely a biztonsági követelményeket és a minősített szerződés elemeinek minősítési szintjével kapcsolatos rendelkezéseket határozza meg. A projekt biztonsági utasítás másolatát azon Szerződő Fél Nemzeti Biztonsági Felügyeletének kell továbbítani, amelynek joghatósága alatt a minősített szerződés teljesítése történik.

5. Jelen Egyezmény alapján megkötött valamennyi minősített szerződésnek tartalmaznia kell:

a) arra irányuló követelményt, hogy a szerződő köteles biztosítani a minősített adathoz hozzáféréssel rendelkező személyek tájékoztatását a minősített adatok védelmével kapcsolatos kötelezettségekről a nemzeti jogszabályokkal összhangban;

b) a minősített adatok, és azon együttműködési területek listája, amely esetén minősített adatok keletkezése, kezelése merülhet fel;

c) a minősített adat minősítési szintjében bekövetkezett változásokról történő tájékoztatás folyamatának leírását;

d) az adat átadásához használt kommunikációs és elektronikus eszközt;

e) a minősített adat átadásának folyamatát;

f) a szerződő értesítési kötelezettségvállalását a minősített adat biztonságának megsértése vagy annak gyanúja esetén;

g) a szerződő a minősített szerződés másolatának saját Nemzeti Biztonsági Felügyeletéhez történő továbbítására vonatkozó kötelezettségvállalást;

h) az alvállalkozó kötelezettségvállalást a szerződőre vonatkozó biztonsági előírások betartására.

9. Cikk

A minősített adat átadása

1. A minősített adat átadása az Átadó Fél nemzeti jogszabályai szerint, diplomáciai úton, vagy a Nemzeti Biztonsági Felügyeletek által közösen meghatározott egyéb módon történik.

2. A Szerződő Felek, a Nemzeti Biztonsági Felügyeletek által 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 minimumra 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!”/ ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ/ TOP SECRET minősítésű adat fordítása vagy sokszorosítása kizárólag az Átadó Fél előzetes írásbeli engedélyével lehetséges.

4. Amennyiben az adat átadásának célja már nem áll fenn a minősített adatot oly módon kell megsemmisíteni, hogy annak se részben, se egészben történő helyreállítása ne legyen lehetséges.

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

6. Olyan veszélyhelyzet esetén, amely lehetetlenné teszi a minősített adat védelmét vagy visszajuttatását, a minősített adatot késedelem nélkül meg kell semmisíteni. Az Átvevő Fél a lehető leghamarabb köteles értesíteni az Átadó Fél Nemzeti Biztonsági Felügyeletét a minősített adat megsemmisítéséről.

7. A minősített adat megsemmisítésére vonatkozó jelentést az Átadó Fél Nemzeti Biztonsági Felügyelete részére szükséges eljuttatni.

11. Cikk

Látogatások

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

2. A Nemzeti Biztonsági Felügyelet a látogatásra vonatkozó megkeresést legalább húsz nappal a látogatás időpontja előtt a másik Szerződő Fél Nemzeti Biztonsági Felügyeletéhez nyújtja be.

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 szükséges részleteit a Nemzeti Biztonsági Felügyeletek közösen állapítják meg. A listák tizenkét hónapig érvényesek.

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

6. Azt követően, hogy a fogadó Szerződő Fél Nemzeti Biztonsági Felügyelete jóváhagyta a látogatást, köteles a nemzeti jogszabályok alapján másolatot biztosítani a látogatási kérelemről a meglátogatandó létesítmény biztonsági vezetőjének.

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 mindezek alapos gyanújáról.

2. Azon Szerződő Fél Nemzeti Biztonsági Felügyelete, ahol a minősített adat biztonságának megsértésére sor került, a nemzeti jogszabályoknak megfelelően, késedelem nélkül intézkedik a minősített adat megsértésének kivizsgálása érdekében vagy kezdeményezi a kivizsgálás lefolytatását. A másik Szerződő Fél Nemzeti Biztonsági Felügyelete megkeresés esetén részt vesz a vizsgálatban.

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

13. Cikk

Költségek viselése

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

14. Cikk

Viták rendezése

Szerződő Felek a jelen Egyezmény értelmezéséből vagy végrehajtásából fakadó vitákat a Szerződő Felek közötti tárgyalás útján, külső igazságszolgáltatási fórum igénybevétele nélkül kötelesek rendezni.

15. cikk

Záró rendelkezések

1. Jelen Egyezmény határozatlan időre jön létre. Jelen Egyezmény a Szerződő 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 Szerződő Felek kölcsönös egyetértésével írásban módosítható. A módosítások hatályba lépésével kapcsolatban az 1. pontban foglaltak az irányadók.

3. Bármelyik Szerződő Fél jogosult jelen Egyezményt bármikor írásban felmondani. Felmondás esetén az Egyezmény a felmondásról szóló írásbeli értesítés másik Szerződő Fél általi kézhezvételétől számított hat 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.

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

Készült Nicosiában, 2015. október 29-én, két eredeti példányban magyar, görög, és angol nyelven, valamennyi szöveg egyaránt hiteles. Eltérő értelmezés esetén az angol nyelvű szöveg az irányadó.

Magyarország Kormánya részéről **A Ciprusi Köztársaság Kormánya részéről”**

”AGREEMENT

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

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

Recognising the important role of the mutual cooperation,

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

Recognising that they ensure equivalent protection for the Classified Information,

Considering the mutual interests in the protection of the exchanged Classified Information, in accordance with the national laws and regulations of the Contracting Parties,

Have agreed as follows:

ARTICLE 1
SCOPE OF THE AGREEMENT

1. The objective of this Agreement is to ensure the mutual protection of all Classified Information, which has been classified by one Contracting Party and transferred to the other Contracting Party or generated in the course of cooperation between the Contracting Parties or between legal entities or individuals under their jurisdiction.

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

ARTICLE 2
DEFINITIONS

For the purpose of this Agreement:

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

b) **“Classified Information”** means any information, regardless of its form or nature, under the national laws and regulations of either Contracting Party, which requires protection against breach of security and has been so designated with a security classification level;

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

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

e) "**National Security Authority**" means the authority of each Contracting Party, which in accordance with its national laws and regulations is responsible for the general implementation and supervision of this Agreement; the respective authorities of the Parties are referred to in Article 3 paragraph 1 of this Agreement;

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

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

h) **"Recipient Party"** means the Contracting Party including legal entities or individuals under its jurisdiction, to which Classified Information of the Originating Party is transferred;

i) **"Third Party"** means any state including legal entities or individuals under its jurisdiction or international organisation which is not a party to this Agreement.

ARTICLE 3
NATIONAL SECURITY AUTHORITIES

1. The National Security Authorities of the Contracting Parties responsible for the general implementation and supervision of this Agreement are:

In Hungary:

Nemzeti Biztonsági Felügyelet/ National Security Authority

In the Republic of Cyprus:

Εθνική Αρχή ΑσφαλείαςΥπουργείο Αμυνας της Κυπριακής Δημοκρατίας/
National Security Authority Ministry of Defence of the Republic of Cyprus

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

3. Upon request the National Security Authorities shall notify each other about other competent authorities.

4. The National Security Authorities shall inform each other of respective national laws and regulations on Classified Information and of any significant amendments thereto and upon request shall exchange information about the security standards, procedures and practices for the protection of Classified Information.

ARTICLE 4
CLASSIFICATION LEVELS AND MARKINGS

The Contracting Parties agree that the following security classification levels are equivalent and correspond to the security classification levels specified in their national laws and regulations:

In Hungary	**In the Republic of Cyprus**	**Equivalent in the English language**
„Szigorúan titkos!”	ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ	TOP SECRET
„Titkos!”	ΑΠΟΡΡΗΤΟ	SECRET
„Bizalmas!”	ΕΜΠΙΣΤΕΥΤΙΚΟ	CONFIDENTIAL
„Korlátozott terjesztésű!”	ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ	RESTRICTED

ARTICLE 5
ACCESS TO CLASSIFIED INFORMATION

Access to Classified Information under this Agreement shall be limited only to individuals on a need-to-know basis who are duly authorised in accordance with the national laws and regulations of the respective Contracting Party to have access to Classified Information of the relevant security classification level.

ARTICLE 6
SECURITY PRINCIPLES

1. In accordance with their national laws and regulations, the Contracting Parties shall take all appropriate measures for the protection of Classified Information, which is exchanged or generated 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 without undue delay of any subsequent changes in the security classification level of the transferred Classified Information.

3. The Recipient Party shall:
a) ensure that Classified Information is marked with equivalent security classification marking in accordance with Article 4;
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 solely for the purpose it has been released for and in accordance with release conditions of the Originating Party.

ARTICLE 7
SECURITY COOPERATION

1. Upon request, the National Security Authorities shall, in accordance with their national laws and regulations, assist each other during the personnel security clearance and facility security clearance procedures.

2. Within the scope of this Agreement, the Contracting Parties shall on request and in accordance with their national laws and regulations, recognise the personnel security clearance certificates and facility security clearance certificates issued by the other Contracting Party.

3. The National Security Authorities shall promptly notify each other about any alteration of the recognised personnel security clearance certificates and facility security clearance certificates, in particular of their withdrawal or downgrading.

4. 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 Contracting 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 Contracting Party to ensure that the measures concerning the protection of Classified Information are still applicable.

3. The Contractor shall submit information about potential sub-contractors in accordance with the national laws and regulations to the National Security Authority in whose territory the Classified Contract is to be implemented.

4. 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 Contracting Party under whose jurisdiction the Classified Contract is to be implemented.

5. Each Classified Contract concluded in accordance with this Agreement shall include:

a) requirement that the Contractor shall ensure that all persons with access to Classified Information are informed of their responsibility towards the protection of Classified Information in accordance with the national laws and regulations;
b) list of Classified Information and list of areas in which Classified Information can arise;
c) procedure for communication of changes in the security classification level of Classified Information;
d) communication means and electronic means for transmission;
e) procedure for the transfer of Classified Information;
f) commitment of the Contractor to notify of any actual or suspected Breach of Security;
g) commitment of the Contractor to forward a copy of the Classified Contract to its own National Security Authority;
h) commitment of the subcontractor to fulfil the same security obligations as the Contractor.

ARTICLE 9
TRANSFER 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 between the National Security Authorities.

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

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 the minimum 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!”/ ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ/ TOP SECRET shall be translated or reproduced only upon the prior written consent of the Originating Party.

4. Classified Information shall be destroyed - after having been recognised as being no longer necessary for the purposes of the transfer - in a manner that prevents its partial or total reconstruction.

5. Classified Information released under this Agreement marked „Szigorúan titkos!"/ ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ/ 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 return Classified Information it shall be destroyed without undue delay. The Receiving Party shall inform the National Security Authority of the Originating Party about this destruction as soon as possible.

7. A report on destruction of Classified Information shall be delivered to the National Security Authority of the Originating Party.

ARTICLE 11
VISITS

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

2. The National Security Authority shall submit the request for visit to the National Security Authority of the other Contracting Party 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. Requests 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; 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. The lists are valid for twelve months.

5. Classified Information acquired by a visitor shall be considered as Classified Information received under this Agreement.

6. Once the visit has been approved by the National Security Authority of the host Contracting Party it shall provide a copy of the request for visit to the security officer of the legal entity to be visited, in accordance with the national laws and regulations.

ARTICLE 12
BREACH OF SECURITY

1. The National Security Authorities shall without undue delay inform each other in writing of a breach of security or suspicion thereof.

2. The National Security Authority of the Contracting Party where the breach of security occurred shall investigate or initiate the investigation of the incident without delay, in accordance with the national laws and regulations. The National Security Authority of the other Contracting Party shall, upon request, co-operate in the investigation.

3. In any case, the National Security Authority of Recipient Party shall inform 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 Contracting Party shall bear its own expenses incurred in the course of the implementation of this Agreement.

ARTICLE 14
SETTLEMENT OF DISPUTES

Any dispute regarding the interpretation or application of this Agreement shall be settled by negotiations between the Contracting Parties, without recourse to outside jurisdiction.

ARTICLE 15
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 Contracting 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 consent of the Contracting Parties in writing. Such amendments shall enter into force in accordance with Paragraph 1.

3. Each Contracting 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 Contracting 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.

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

Done in Nicosia on 29th October 2015 in two originals, each in Hungarian, Greek 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 Cyprus"

4. §

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

(2) A 2. § és a 3. § az Egyezmény 15. 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 CIPRUSI 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 Ciprusi Köztársaság Kormánya között a minősített adatok cseréjéről és kölcsönös védelméről szóló egyezmény létrehozására, amelyet a felek 2015. október 29-én, Nicosiában 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 15. Cikk 1. bekezdése szerint az Egyezmény „azt a napot követő második hónap első napján lép hatályba, amikor jelen Egyezmény hatálybalépéshez szükséges belső eljárások véghezviteléről szóló értesítéseket a Felek kézhez vették”. 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.