

**MAGYARORSZÁG KORMÁNYA**

**T/2918. számú**

**törvényjavaslat**

**Magyarország Kormánya és az Albán Köztársaság Minisztertanácsa 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 az Albán Köztársaság Minisztertanácsa között a minősített adatok cseréjéről és kölcsönös védelméről szóló egyezmény kihirdetéséről****1. §**

Az Országgyűlés e törvénnyel felhatalmazást ad a Magyarország Kormánya és az Albán Köztársaság Minisztertanácsa 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, albán és angol nyelvű szövege a következő:

”

**EGYEZMÉNY**

**Magyarország Kormánya és az Albán Köztársaság Minisztertanácsa**

**között**

**a minősített adatok cseréjéről és kölcsönös védelméről**

Magyarország Kormánya és az Albán Köztársaság Minisztertanácsa

(a továbbiakban együtt: Felek)

Elismerve a kölcsönös együttműködés fontos szerepét,

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,

Az alábbiakban állapodtak meg:

## **1. CIKK**

### **AZ EGYEZMÉNY TÁRGYA**

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. 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 jogosulatlan hozzáféréssel vagy jogosulatlan megváltoztatással szemben, s amelyet ennek megfelelően minősítettek.
- b)* A „**Minősített Szerződés**” olyan szerződést jelent, amely minősített adatot tartalmaz vagy amely alapján minősített adathoz való hozzáférés szükséges.
- c)* Az „**Átadó Fél**” azt a Felet, valamint a joghatósága alá tartozó jogi személyeket vagy természetes személyeket jelenti, amelyik a minősített adatot átadja.
- d)* Az „**Átvevő Fél**” azt a Felet, valamint a joghatósága alá tartozó jogi személyeket vagy természetes személyeket jelenti, amelyik a minősített adatot átveszi.

- e) 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.
- f) A „**Személyi Biztonsági Tanúsítvány**” valamely Fél állampolgára részére a hatáskörrel rendelkező biztonsági hatóság által a nemzeti jogszabályokkal összhangban a minősített adathoz történő hozzáférés érdekében kiállított tanúsítvány.
- g) A „**Telephely Biztonsági Tanúsítvány**” valamely hatáskörrel rendelkező biztonsági hatóság által kiállított olyan tanúsítvány, mely igazolja, hogy az érintett cég/ létesítmény biztonsági szempontú átvilágítása a nemzeti jogszabályokkal összhangban megtörtént.
- h) A „**Szükséges Ismeret elve**” azt a követelményt jelenti, amely alapján a minősített adathoz történő hozzáférés csak olyan személy részére biztosítható, akinek a hozzáférés hivatali feladata ellátásához szükséges.
- i) A „**Látogató**” valamely Fél azon hivatalos képviselője, aki kezdeményezi a másik Fél joghatósága alá tartozó, minősített adatot érintő tevékenységet végző intézmény meglátogatását.

### 3. CIKK

#### A HATÁSKÖRREL RENDELKEZŐ BIZTONSÁGI HATÓSÁGOK

1. Felek a minősített adatok védelméért, valamint jelen Egyezmény végrehajtásáért felelős, hatáskörrel rendelkező biztonsági hatóságai a következők:

Magyarországon:

Nemzeti Biztonsági Felügyelet

Az Albán Köztársaságban:

Drejtoria e Sigurimit te Informacionit te Klasifikuar (Minősített Adatvédelmi Igazgatóság-Nemzeti Biztonsági Felügyelet)

2. A hatáskörrel rendelkező biztonsági hatóságok kölcsönösen tájékoztatják egymást a hivatalos elérhetőségi adatokról, illetve az ezen adatokkal kapcsolatos változásokról.

**4. CIKK****MINŐSÍTÉSI SZINTEK MEGFELELTETÉSE**

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

<b>MAGYARORSZÁGON</b>	<b>AZ ALBÁN KÖZTÁRSASÁGBAN</b>	<b>ANGOL NYELVŰ MEGFELELŐJÜK</b>
„Szigorúan titkos!”	Tepër Sekret	TOP SECRET
„Titkos!”	Sekret	SECRET
„Bizalmas!”	Konfidencial	CONFIDENTIAL
„Korlátozott terjesztésű!”	I Kufizuar	RESTRICTED

**5. CIKK****MINŐSÍTETT ADATHOZ VALÓ HOZZÁFÉRÉS**

Minősített adathoz jelen Egyezmény alapján kizárólag olyan személyek jogosultak hozzáférni, akik az adott 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 minősítésében 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 az átvett 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 meghatározott kezelési előírásokat.

## 7. CIKK

### BIZTONSÁGI EGYÜTTMŰKÖDÉS

1. A hasonló szintű biztonsági követelmények fenntartása érdekében a hatáskörrel rendelkező biztonsági hatóságok a másik fél megkeresésére kötelesek egymást tájékoztatni a minősített adat védelmével kapcsolatos nemzeti jogszabályokról, azok lényeges változásairól, valamint mindezek gyakorlati alkalmazásáról.

2. Megkeresés esetén a hatáskörrel rendelkező biztonsági hatóságok, összhangban a nemzeti jogszabályaik rendelkezéseivel, kölcsönösen segítséget nyújtanak egymásnak a személyi biztonsági tanúsítványokkal és a telephely biztonsági tanúsítványokkal kapcsolatos eljárások során.

3. A Felek megkeresés esetén nemzeti jogszabályaik rendelkezéseivel összhangban elismerik a másik Fél által kibocsátott személyi biztonsági tanúsítványokat és telephely biztonsági tanúsítványokat.

4. A hatáskörrel rendelkező biztonsági hatóságok haladéktalanul értesítik egymást az elismert személyi biztonsági tanúsítványokkal és a telephely biztonsági tanúsítványokkal kapcsolatos változásokról, különösen azok visszavonásáról vagy leminősítéséről.

## **8. CIKK**

### **MINŐSÍTETT SZERZŐDÉSEK**

1. A minősített szerződéseket a Felek saját nemzeti jogszabályai alapján kell megkötni és teljesíteni. A hatáskörrel rendelkező biztonsági hatóságok megkeresésre 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 hatáskörrel rendelkező biztonsági hatóságok 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 hatáskörrel rendelkező biztonsági hatósága 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 hatáskörrel rendelkező biztonsági hatóságok által végrehajtási utasításokban közösen meghatározott egyéb módon történik. Az Átvevő Fél írásban köteles megerősíteni a minősített adat átvételének megtörténtét.

2. A Felek, a hatáskörrel rendelkező biztonsági hatóságok által jóváhagyott eljárási rend szerint, elektronikus úton is továbbíthatnak minősített adatot.

## 10. CIKK

### A MINŐSÍTETT ADAT SOKSZOROSÍTÁSA, FORDÍTÁSA ÉS MEGSEMISÍTÉSE

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!”/ Tepër Sekret/ TOP SECRET minősítésű adat fordítása vagy sokszorosítása kizárólag az Átadó Fél előzetes írásbeli engedélyével lehetséges.
4. Ha a továbbítás célja már nem áll fenn, akkor a minősített adatot oly módon kell megsemmisíteni, hogy annak teljes vagy részleges helyreállítása ne legyen lehetséges. A megsemmisítésről az Átadó Felet, amint lehetséges értesíteni kell.
5. Jelen Egyezmény alapján átadott, „Szigorúan titkos!”/ Tepër Sekret/ TOP SECRET minősítésű adat nem semmisíthető meg, az ezen minősítési szintű adatokat az Átadó Félnek kell visszaszolgáltatni.
6. 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.

## 11. CIKK

### LÁTOGATÁSOK

1. Minősített adathoz való hozzáférést igénylő látogatásra az érintett hatáskörrel rendelkező biztonsági hatóság előzetes írásbeli jóváhagyása alapján kerülhet sor.
2. A látogatásra vonatkozó megkeresést legalább húsz nappal a látogatás időpontja előtt a hatáskörrel rendelkező biztonsági hatósághoz kell benyújtani, amely továbbítja azt a másik Fél hatáskörrel rendelkező biztonsági hatóságához. Sürgős esetben a hatáskörrel rendelkező



biztonsági hatóságok 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 intézmény 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 hatáskörrel rendelkező biztonsági hatóság hivatalos pecsétjének lenyomata.

4. A hatáskörrel rendelkező biztonsági hatóságok közösen meghatározhatják a visszatérő látogatásra jogosult személyek listáját. A visszatérő látogatások további részleteit a hatáskörrel rendelkező biztonsági hatóságok 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 hatáskörrel rendelkező biztonsági hatóságok késedelem nélkül írásban tájékoztatják egymást a minősített adat biztonságának megsértéséről, amely esetben a jelen Egyezmény hatálya alá tartozó minősített adathoz való jogosulatlan hozzáférésre, nyilvánosságra

hozatalra, a minősített adat jogosulatlan megváltoztatására, megsemmisítésére, elvesztésre, vagy bármilyen más kompromittálódására kerül sor, vagy mindezek alapos gyanúja merül fel.

2. Azon Fél hatáskörrel rendelkező biztonsági hatósága, ahol a minősített adat biztonságának megsértésére sor került, késedelem nélkül intézkedik a minősített adat megsértésének kivizsgálása érdekében. A másik Fél hatáskörrel rendelkező biztonsági hatósága szükség esetén részt vesz a vizsgálatban.

3. Az Átvevő Fél hatáskörrel rendelkező biztonsági hatósága 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 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 Szerződő 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 Szerződő 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 Budapesten, 2014. szeptember 8-án, két eredeti példányban, magyar, albán és angol nyelven, mindhárom szöveg egyaránt hiteles. Eltérés esetén az angol nyelvű szöveg az irányadó.

MAGYARORSZÁG KORMÁNYA  
RÉSZÉRŐL

AZ ALBÁN KÖZTÁRSASÁG  
MINISZTERTANÁCSA RÉSZÉRŐL

## **MARRËVESHJE**

**ndërmjet**

**Qeverisë së Hungarisë**

**dhe Këshillit të Ministrave të Republikës së Shqipërisë**

**mbi shkëmbimin dhe mbrojtjen reciproke**

**të informacionit të klasifikuar**

Qeveria e Hungarisë dhe Këshilli i Ministrave i Republikës së Shqipërisë

(më poshtë të quajtura "Palët"),

Duke njohur rolin e rëndësishëm të bashkëpunimit reciprok;

Duke qenë të ndërgjegjshëm se bashkëpunimi i mirë kërkon shkëmbimin e Informacionit të Klasifikuar ndërmjet Palëve,

Duke njohur se ato sigurojnë mbrojtje të barasvlershme të Informacionit të Klasifikuar,

Me dëshirën për të siguruar mbrojtjen e Informacionit të Klasifikuar të shkëmbyer ndërmjet tyre ose ndërmjet subjekteve juridike ose individëve nën juridiksionin e tyre,

Kanë rënë dakord sa më poshtë:

## NENI 1

### OBJEKTI I MARRËVESHJES

Synimi i kësaj Marrëveshjeje është sigurimi i mbrojtjes së Informacionit të Klasifikuar të shkëmbyer ose të gjeneruar në kuadrin e bashkëpunimit ndërmjet Palëve ose subjekteve juridike apo individëve nën juridiksionin e tyre.

## NENI 2

### PËRKUFIZIME

Për qëllimet e kësaj Marrëveshjeje:

- a) "**Informacion i Klasifikuar**" është çdo informacion që pavarësisht nga forma ose natyra e tij, në bazë të legjislacionit të brendshëm të një Pale, kërkon mbrojtje ndaj deklarimit të paautorizuar ose një manipulimi tjetër të paautorizuar dhe që është përcaktuar rregullisht.
- b) "**Kontratë e Klasifikuar**" është një kontratë që përfshin ose kërkon akses në Informacionin e Klasifikuar;
- c) "**Palë e Origjinës**" është Pala, duke përfshirë subjektet juridike ose individët nën juridiksionin e saj, e cila nxjerr Informacionin e Klasifikuar.
- d) "**Palë Marrëse**" është Pala, duke përfshirë subjektet juridike ose individët nën juridiksionin e saj, e cila merr Informacionin e Klasifikuar.
- e) "**Palë e Tretë**" është çdo shtet, duke përfshirë subjektet juridike ose individët nën juridiksionin e tij ose një organizatë ndërkombëtare, që nuk është palë në këtë Marrëveshje.
- f) "**Leje Sigurie Personeli**" është certifikata e dhënë nga Autoriteti Kompetent i Sigurisë për një shtetas të një Pale për akses tek Informacioni i Klasifikuar, në pajtim me legjislacionin e brendshëm.

- g) "**Leje Sigurie Struktore**" është certifikata e dhënë nga Autoriteti Kompetent i Sigurisë që përcakton se një shoqëri/strukturë është me leje sigurie për të trajtuar Informacionin e Klasifikuar, në pajtim me ligjet dhe rregulloret përkatëse të brendshme.
- h) "**Nevoja për të ditur**" është një parim, i cili synon aksesin në Informacionin e Klasifikuar. Ky informacion lejohet vetëm për individët që kanë një nevojë për të verifikuar Informacionin e Klasifikuar në lidhje me përmbushjen e detyrave të tyre zyrtare.
- i) "**Vizitorë**" janë përfaqësues zyrtarë të një Pale që kërkojnë të vizitojnë mjediset e Palës tjetër të përfshirë në aktivitete që lidhen me Informacionin e Klasifikuar.

### NENI 3

#### AUTORITETET KOMPETENTE TË SIGURISË

1. Autoritetet Kompetente të Sigurisë së Palëve përgjegjëse për mbrojtjen e Informacionit të Klasifikuar si dhe zbatimin e kësaj Marrëveshjeje janë:

Në Hungari:

Autoriteti i Sigurisë Kombëtare; Nemzeti Biztonsági Felügyelet

Në Republikën e Shqipërisë:

Drejtoria e Sigurimit të Informacionit të Klasifikuar (Autoriteti i Sigurisë Kombëtare)

2. Autoritetet Kompetente të Sigurisë i japin njëri-tjetrit të dhënat e kontaktit zyrtar dhe njoftojnë njëri-tjetrin për çdo ndryshim të mëvonshëm të tyre.

### NENI 4

#### NIVELET DHE SHËNJIMET E KLASIFIKIMIT TË SIGURISË

Barazvlershmëria e niveleve dhe shënimeve të klasifikimit të sigurisë kombëtare është si më poshtë:

NË HUNGARI	NË REPUBLIKËN E SHQIPËRISË	EKUIVALENTI NË GJUHËN ANGLEZE
„Szigorúan titkos!”	Tepër Sekret	TOP SECRET

„Titkos!”	Sekret	SECRET
„Bizalmas!”	Konfidencial	CONFIDENTIAL
„Korlátozott terjesztésű!”	I Kufizuar	RESTRICTED

## NENI 5

### AKSESI NË INFORMACIONIN E KLASIFIKUAR

Aksesi në Informacionin e Klasifikuar sipas kësaj Marrëveshjeje lejohet vetëm për individët e autorizuar rregullisht në pajtim me ligjet dhe rregulloret e brendshme të Palës përkatëse.

## NENI 6

### PARIMET E SIGURISË

#### 1. Pala e Origjinës:

- a) siguron që Informacioni i Klasifikuar të shënjohej me shënimet e duhura të klasifikimit të sigurisë, në pajtim me legjislacionin e brendshëm;
- b) informon Palën Pritëse për çdo kusht në përdorimin e Informacionit të Klasifikuar;
- c) informon Palën Pritëse pa vonesë për çdo ndryshim të mëvonshëm në nivelin e klasifikimit të sigurisë.

#### 2. Pala Marrëse:

- a) siguron që Informacioni i Klasifikuar të Shënjohej me shënjimete e barasvlershme të klasifikimit të sigurisë në pajtim me Nenin 4;
- b) ofron të njëjtën shkallë mbrojtjeje të Informacionit të Klasifikuar që i jepet Informacionit të saj të Klasifikuar me nivel të barasvlershëm të klasifikimit të sigurisë;
- c) siguron që Informacioni i Klasifikuar të mos deklasifikohet dhe niveli i klasifikimit të sigurisë të mos ndryshohet pa pëlqimin paraprak me shkrim të Palës së Origjinës;
- d) siguron që Informacioni i Klasifikuar të mos i jepet një Pale të Tretë pa pëlqimin paraprak me shkrim të Palës së Origjinës;
- e) e përdor Informacionin e Klasifikuar vetëm për qëllimin që është dhënë dhe në pajtim me kushtet e dhënies nga Pala e Origjinës.

**NENI 7****BASHKËPUNIMI PËR SIGURINË**

1. Me qëllim që të ruhen standardet e krahasueshme të sigurisë, Autoritetet Kompetente të Sigurisë njoftojnë me shkrim njëra-tjetrën për ligjet dhe rregulloret e tyre të brendshme dhe çdo ndryshim të rëndësishëm në lidhje me mbrojtjen e Informacionit të Klasifikuar dhe praktikatat që rrjedhin nga zbatimi i tyre.
2. Me kërkesë, Autoritetet Kompetente të Sigurisë, në pajtim me ligjet dhe rregulloret e tyre të brendshme, ndihmojnë njëri-tjetrin gjatë procedurave të Lejeve të Sigurisë së Personelit dhe Procedurave të Lejeve të Sigurisë së Strukturës.
3. Palët, me kërkesë dhe në pajtim me ligjet dhe rregulloret e tyre të brendshme, njohin Certifikatat e Lejeve të Sigurisë së Personelit dhe certifikatat e Lejeve të Sigurisë së Strukturës të lëshuara nga Pala tjetër.
4. Autoritetet Kompetente të Sigurisë njoftojnë menjëherë njëri-tjetrin në lidhje me ndryshimet në certifikatat e njohura të Lejeve të Sigurisë së Personelit dhe certifikatat e Lejeve të Sigurisë së Strukturës, veçanërisht në rastin e tërheqjes ose uljes së nivelit të tyre.

**NENI 8****KONTRATAT E KLASIFIKUARA**

1. Kontratat e Klasifikuara lidhen dhe zbatohen në pajtim me ligjet dhe rregulloret e brendshme të secilës Palë. Me kërkesë, Autoritetet Kompetente të Sigurisë konfirmojnë që kontraktorët e propozuar si dhe individët që marrin pjesë në bisedimet para-kontraktuale ose në zbatimin e Kontratave të Klasifikuara, të kenë certifikata të përshtatshme të Lejeve të Sigurisë së Personelit dhe certifikata të Lejeve të Sigurisë së Strukturës.
2. Autoriteti Kompetent i Sigurisë mund t'i kërkojë homologut të tij që të kryhet një inspektim sigurie në një strukturë të vendosur jashtë territorit të Palës tjetër për të siguruar mbrojtjen e vazhdueshme të Informacionit të Klasifikuar.
3. Kontratat e Klasifikuara përmbajnë udhëzime për sigurinë e projektit mbi kërkesat e sigurisë dhe nivelin e klasifikimit të sigurisë të çdo elementi të Kontratës së Klasifikuar. Një kopje e udhëzimeve të sigurisë së projektit i paraqitet Autoritetit Kompetent të Sigurisë të palës nën juridiksionin e të cilit zbatohet Kontrata e Klasifikuar.

**NENI 9****TRANSFERIMI I INFORMACIONIT TË KLASIFIKUAR**

1. Informacioni i Klasifikuar përcillet në pajtim me ligjet dhe rregulloret e brendshme të Palës së Origjinës nëpërmjet kanaleve diplomatike ose siç bihet dakord ndryshe ndërmjet Autoriteteve Kompetente të Sigurisë në protokollet ekzekutive. Pala Pritëse konfirmon me shkrim marrjen e Informacionit të Klasifikuar.
2. Palët mund të transmetojnë Informacion të Klasifikuar me mjete elektronike në pajtim me procedurat e sigurisë të miratuara nga Autoritetet Kompetente të Sigurisë.

**NENI 10****RIPRODHIMI, PËRKTHIMI DHE ASGJËSIMI I INFORMACIONIT TË KLASIFIKUAR**

1. Riprodhimet dhe përkthimet e Informacionit të Klasifikuar të dhëna sipas kësaj Marrëveshjeje kanë shënimet e përshtatshme të klasifikimit të sigurisë dhe mbrohen si origjinalet. Numri i kopjeve kufizohet tek ai që kërkohet për qëllime zyrtare.
2. Përkthimet e Informacionit të Klasifikuar të dhëna sipas kësaj Marrëveshjeje kanë një shënim në gjuhën e përkthimit që tregon se ato përmbajnë Informacion të Klasifikuar të Palës së Origjinës.
3. Informacioni i Klasifikuar i dhënë sipas kësaj Marrëveshjeje, i shënuar „Szigorúan titkos!”/ Tepër Sekret/ TOP SECRET përkthehet ose riprodhohet vetëm me pëlqimin paraprak me shkrim të Palës së Origjinës.
4. Informacioni i Klasifikuar asgjësohet pasi konfirmohet që nuk vazhdon të mbetet i nevojshëm për qëllimet e transferimit, në një mënyrë që përjashton rindërtimin e tij të pjesshëm ose të plotë. Pala e Origjinës njoftohet në lidhje me asgjësimin sa më shpejt të jetë e mundur.
5. Informacioni i Klasifikuar i dhënë sipas kësaj Marrëveshjeje, i shënuar „Szigorúan titkos!”/ Tepër Sekret/ TOP SECRET nuk asgjësohet por i kthehet Palës së Origjinës.
6. Në rastin e një situatë krize në të cilën nuk është e mundur mbrojtja ose kthimi i Informacionit të Klasifikuar tek Pala e Origjinës, ai asgjësohet menjëherë.

**NENI 11****VIZITAT**

1. Vizitat që kërkojnë akses në Informacionin e Klasifikuar i nënshtrohen pëlqimit paraprak me shkrim të Autoritetit përkatës Kompetent të Sigurisë.



2. Kërkesat për vizitë i paraqiten Autoritetit Kompetent të Sigurisë jo më vonë se njëzet ditë para kryerjes së vizitës, i cili ia kalon atë Autoritetit Kompetent të Sigurisë të Palës tjetër. Në raste urgjente, kërkesa për vizitë i nënshtrohet bashkërendimit të drejtpërdrejtë ndërmjet autoriteteve kompetente të sigurisë.

3. Kërkesat për vizitë përmbajnë:

- a) emrin, datën dhe vendin e lindjes, shtetësinë dhe numrin e pasaportës/kartës së identitetit të vizitorit;
- b) pozicionin e vizitorit dhe specifikimin e subjektit juridik që përfaqësohet;
- c) statusin e certifikatës së lejes së sigurisë së personelit për vizitorin dhe vlefshmërinë e saj;
- d) datën dhe kohëzgjatjen e vizitës; në rastin e vizitave periodike, periudhën e plotë kohore që mbulohet nga vizitat;
- e) qëllimin e vizitës, duke përfshirë nivelin më të lartë të klasifikimit të sigurisë të Informacionit të Klasifikuar përkatës;
- f) emrin dhe adresën e strukturës që vizitohet, si dhe emrin, numrin e telefonit/faksit, adresën e e-mail-it ose pikën e tij të kontaktit;
- g) datën, nënshkrimin dhe vulën zyrtare të Autoritetit Kompetent të Sigurisë.

4. Autoritetet Kompetente të Sigurisë mund të bien dakord për një listë vizitorësh që kanë të drejtën e vizitave periodike. Autoritetet Kompetente të Sigurisë bien dakord për të dhënat e mëtejshme të vizitave periodike.

5. Informacioni i Klasifikuar i përftuar nga një vizitor konsiderohet si Informacion i Klasifikuar i marrë sipas kësaj Marrëveshjeje.

## **NENI 12**

### **SHKELJA E SIGURISË**

1. Autoritetet Kompetente të Sigurisë njoftojnë njëri-tjetrin me shkrim pa vonesë për shkeljen e sigurisë që sjell një deklaram të pa-autorizuar, humbje, asgjësim, përftim të papërshtatshëm ose një lloj tjetër cenimi të Informacionit të Klasifikuar të shkëmbyer ose të gjeneruar sipas kësaj Marrëveshjeje ose dyshimi për të.

2. Autoriteti Kompetent i Sigurisë së Palës ku ka ndodhur shkelja e sigurisë fillon hetimin e incidentit pa vonesë. Nëse kërkohet, Autoriteti tjetër Kompetent për Sigurinë bashkëpunon në hetim.

3. Në çdo rast, Autoriteti Kompetent i Sigurisë i Palës Marrëse njofton me shkrim Palën e Origjinës në lidhje me rrethanat e shkeljes së sigurisë, masën e dëmit, masat e marra për zbutjen e tij dhe rezultatin e hetimit.

### **NENI 13**

#### **SHPENZIMET**

Secila Palë mbulon shpenzimet e veta të bëra gjatë zbatimit të kësaj Marrëveshjeje.

### **NENI 14**

#### **DISPOZITA TË FUNDIT**

1. Kjo Marrëveshje lidhet për një periudhë të pacaktuar kohe dhe hyn në fuqi në ditën e parë të muajit të dytë pas datës së marrjes së njoftimit të fundit ndërmjet Palëve, nëpërmjet kanaleve diplomatike, i cili përcakton se procedurat e brendshme ligjore për hyrjen në fuqi të kësaj Marrëveshjeje, janë përbushur.

2. Kjo Marrëveshje mund të ndryshohet mbi bazën e pëlqimit reciprok me shkrim të Palëve. Këto ndryshime hyjnë në fuqi në pajtim me paragrafin 1 të këtij neni.

3. Secila Palë ka të drejtë ta prishë këtë Marrëveshje me shkrim në çdo kohë. Në një rast të tillë, vlefshmëria e kësaj Marrëveshjeje skadon pas gjashtë muajsh pas datës në të cilën Pala tjetër merr njoftimin me shkrim për zgjidhjen e kësaj marrëveshjeje.

4. Pavarësisht prishjes së Marrëveshjes, i gjithë Informacioni i Klasifikuar, i shkëmbyer ose i gjeneruar sipas kësaj Marrëveshje mbrohet në pajtim me dispozitat e parashikuara në këtë Marrëveshje, derisa Pala e Origjinës ta lirojë Palën Marrëse nga ky detyrim me shkrim.

5. Çdo mosmarrëveshje në lidhje me interpretimin ose zbatimin e kësaj Marrëveshjeje zgjidhet me konsultime dhe bisedime ndërmjet Palëve, pa iu drejtuar juridiksionit të jashtëm.

Në dëshmi të kësaj, të nënshkruarit, duke qenë të autorizuar sipas rregullave nga Qeveritë e tyre përkatëse, kanë nënshkruar këtë Marrëveshje.

Bërë në Budapest, më 8 Shtator 2014, në dy kopje origjinale, në gjuhët shqipe, hungareze dhe angleze, ku secili tekst është njëlloj i vlefshëm. Në rastin e mospërputhjes në interpretim, teksti në gjuhën angleze do të ketë përparësi.

**PËR QEVERINË E HUNGARISË**

**PËR KËSHILLIN E MINISTRAVE  
TË REPUBLIKËS SË  
SHQIPËRISË**

**AGREEMENT**

**between the Government of Hungary  
and the Council of Ministers of the Republic of Albania  
on the Exchange and Mutual Protection  
of Classified Information**

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

Recognising the important role of the mutual co-operation,

Realising that good co-operation 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 legal entities or individuals under their jurisdiction,

Have agreed upon the following:

**ARTICLE 1**

**SCOPE OF THE AGREEMENT**

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 legal entities or individuals under their jurisdiction.

**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 legislation of either Party, requires protection against unauthorised disclosure or any other unauthorised manipulation and has been duly designated.
- b) **“Classified Contract”** means a contract that involves or requires access to Classified Information.
- c) **“Originating Party”** means the Party including legal entities or individuals under its jurisdiction, which releases Classified Information.
- d) **“Recipient Party”** means the Party including legal entities or individuals under its jurisdiction, which receives Classified Information.
- e) **“Third Party”** means any state including legal entities or individuals under its jurisdiction or international organisation not being a party to this Agreement.
- f) **"Personnel Security Clearance"** means the certificate granted by the Competent Security Authority to a national of a Party for access to Classified Information, in accordance with the respective national laws and regulations.
- g) **"Facility Security Clearance"** means the certificate granted by the Competent Security Authority providing that a company/ establishment is security cleared to handle Classified Information, in accordance with the respective national laws and regulations.
- h) **"Need-to-know"** means a principle by which access to Classified Information may only be granted to individuals who have a verified need to access this Classified Information in connection with the performance of their official duties or tasks.
- i) **"Visitors"** means the official representatives of one Party who require to visit premises of the other Party engaged in activities involving Classified Information.

**ARTICLE 3****COMPETENT SECURITY AUTHORITIES**

1. The Competent Security Authorities of the Parties responsible for the protection of Classified Information as well as the implementation of this Agreement are:

In Hungary:

National Security Authority

Nemzeti Biztonsági Felügyelet

In the Republic of Albania:

Classified Information Security Directorate (National Security Authority)

Drejtoria e Sigurimit te Informacionit te Klasifikuar

2. The Competent 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:

<b>IN HUNGARY</b>	<b>IN THE REPUBLIC OF ALBANIA</b>	<b>EQUIVALENT IN THE ENGLISH LANGUAGE</b>
„Szigorúan titkos!”	Tepër Sekret	TOP SECRET
„Titkos!”	Sekret	SECRET
„Bizalmas!”	Konfidencial	CONFIDENTIAL
„Korlátozott terjesztésű!”	I Kufizuar	RESTRICTED

**ARTICLE 5****ACCESS TO CLASSIFIED INFORMATION**

Access to Classified Information under this Agreement shall be limited only to individuals 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;
- b) afford the same degree of protection to Classified Information as afforded to its own Classified Information of equivalent security classification level;
- c) ensure that Classified Information is not declassified nor its security classification level changed without the prior written consent of the Originating Party;
- d) ensure that Classified Information is not released to a Third Party without the prior written consent of the Originating Party;
- e) use Classified Information only for the purpose it has been released for and in accordance with release conditions of the Originating Party.

**ARTICLE 7****SECURITY CO-OPERATION**

1. In order to maintain comparable standards of security, the Competent Security Authorities shall, on request, inform each other of their national laws and regulations and any significant amendments concerning protection of Classified Information and the practices stemming from their implementation.
2. On request, the Competent 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. The 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 Party.
4. The Competent 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 or downgrading.

**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 Competent 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 Competent 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 Competent Security Authority of the Party under whose jurisdiction the Classified Contract is to be implemented.

## **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 Competent Security Authorities in executive protocols. The Recipient Party shall confirm the receipt of Classified Information in writing.
2. The Parties may transmit Classified Information by electronic means in accordance with the security procedures approved by the Competent 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 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 as „Szigorúan titkos!”/ Tepër Sekret/ 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. The Originating Party shall be informed about the destruction as soon as possible.



5. Classified Information released under this Agreement marked as „Szigorúan titkos!”/ Top Secret/ TOP SECRET shall not be destroyed but shall be returned to the Originating Party.

6. In case of a crisis situation, in which it is impossible to protect or return the Classified Information to the Originating Party, it shall be destroyed without undue delay.

## **ARTICLE 11**

### **VISITS**

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

2. Requests for visit at least twenty days before the visit takes place shall be submitted to the Competent Security Authorities which shall forward it to the Competent Security Authority of the other Party. In urgent cases, the request for visit may be submitted at a shorter notice, subject to prior co-ordination between the Competent 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 Competent Security Authority.

4. The Competent Security Authorities may agree on a list of visitors entitled to recurring visits. The Competent 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 Competent Security Authorities shall inform each other in writing without undue delay of a breach of security resulting in unauthorised disclosure, loss, destruction, misappropriation or any other type of compromise of Classified Information exchanged or generated under this Agreement or suspicion thereof.

2. The Competent Security Authority of the Party, where the breach of security occurred, shall initiate the investigation of the incident without undue delay. The other Competent Security Authority shall, if required, co-operate in the investigation.

3. In any case, the Competent Security Authority of the 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 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.
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 Budapest on 8 September 2014 in two originals, in Hungarian, Albanian 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 COUNCIL OF  
MINISTERS OF THE REPUBLIC  
OF ALBANIA”

**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 AZ ALBÁN KÖZTÁRSASÁG  
MINISZTERTANÁCSA KÖZÖTT A MINŐSÍTETT ADATOK CSERÉJÉRŐL ÉS KÖLCSÖNÖS  
VÉDELMEÉRŐL 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, albán 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.