MAGYARORSZÁG KORMÁNYA

T/13088. számú

törvényjavaslat

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

Előadó: **Dr. Pintér Sándor**
belügyminiszter

Budapest, 2016. november

2016. évi … törvény

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

1. §

Az Országgyűlés e törvénnyel felhatalmazást ad a Magyarország Kormánya és Montenegró 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 MONTENEGRÓ KORMÁNYA KÖZÖTT
A MINŐSÍTETT ADATOK CSERÉJÉRŐL ÉS KÖLCSÖNÖS VÉDELMÉRŐL

Magyarország Kormánya és Montenegró Kormánya (a továbbiakban: Felek)
Elismerve a Felek közötti kölcsönös együttműködés jelentőségét,
Felismerve, hogy a Felek közötti jó együttműködés során szükség lehet minősített adatok cseréjére,
Elismerve, hogy azonos szintű védelmet biztosítanak a minősített adatok számára,
Kívánatosnak tartva, hogy a közöttük vagy joghatóságuk alá tartozó jogi személyek vagy természetes személyek között kicserélt minősített adatok megfelelő védelemben részesüljenek,
Kölcsönösen tiszteletben tartva a nemzeti érdekeket és a biztonságot, az alábbiakban állapodtak meg:

1. CIKK

AZ EGYEZMÉNY CÉLJA ÉS ALKALMAZÁSI TERÜLETE

Jelen Egyezmény célja, hogy védelmet biztosítson a Felek, valamint joghatóságuk alá tartozó jogi személyek vagy természetes személyek közötti együttműködés során kicserélt vagy keletkezett minősített adatok számára.

2. CIKK

FOGALOM-MEGHATÁROZÁSOK

Jelen Egyezmény alkalmazásában:
a) **a minősített adat biztonságának megsértése**: olyan, jelen Egyezménnyel vagy a Felek nemzeti jogszabályaival és egyéb szabályainak rendelkezéseivel ellentétes tevékenység vagy mulasztás, ami

a minősített adat jogosulatlan nyilvánosságra hozatalához, elvesztéséhez, megsemmisüléséhez, jogosulatlan felhasználásához, megszerzéséhez vagy egyéb módon történő megsértéséhez vezethet;

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

c) **minősített ada**t: megjelenési formájától, természetétől függetlenül minden olyan adat, amelyet bármelyik Fél nemzeti jogszabályai és egyéb szabályainak rendelkezései szerint védelemben kell részesíteni a minősített adat biztonságának megsértésével szemben, és amelyet ennek megfelelően minősítettek;

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

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

f) **nemzeti biztonsági hatóság**: az az állami szerv, amely jelen Egyezmény alkalmazásáért és felügyeletéért felelős;

g) **szükséges ismeret**: az a követelmény, amely alapján a minősített adathoz való hozzáférés csak annak a személynek biztosítható, akinek az adott minősített adathoz való hozzáférés hivatali kötelessége vagy meghatározott feladata ellátásához igazoltan szükséges;

h) **átadó fél:** az a Fél – beleértve a joghatósága alá tartozó jogi személyeket, egyéb szervezeti egységeket vagy természetes személyeket –, amelyik a nemzeti minősített adatot átadja;

i) **személyi biztonsági tanúsítvány**: a nemzeti biztonsági hatóság azon döntése, amely szerint egy természetes személy a nemzeti jogszabályok és egyéb szabályok rendelkezéseivel összhangban jogosult hozzáférni minősített adatokhoz;

j) **átvevő fél:** az a Fél – beleértve a joghatósága alá tartozó jogi személyeket, egyéb szervezeti egységeket vagy természetes személyeket –, amelyik a nemzeti minősített adatot átveszi;

k) **alvállalkozói szerződés:** a szerződő által, egy másik szerződővel (alvállalkozóval) kötött, termékek szolgáltatására vagy szolgáltatások nyújtására irányuló szerződés;

l) **alvállalkozó:** olyan természetes személy vagy jogi személy, aki a szerződővel az alvállalkozói szerződést megköti;

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

3. CIKK

NEMZETI BIZTONSÁGI HATÓSÁGOK

(1) A Felek nemzeti biztonsági hatóságai:
Magyarországon:
Nemzeti Biztonsági Felügyelet
Montenegróban:
Minősített Adatvédelmi Igazgatóság (Nemzeti Biztonsági Felügyelet)
Direkcija za zaštitu tajnih podataka

(2) A nemzeti biztonsági hatóságok tájékoztatják egymást hivatalos elérhetőségi adataikról, és a nemzeti biztonsági hatóságokkal kapcsolatos valamennyi későbbi változásról.

4. CIKK

MINŐSÍTÉSI SZINTEK ÉS JELÖLÉSEK

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

Magyarországon	**Montenegróban**	**Angol nyelvű megfelelőjük**
„Szigorúan titkos!”	“STROGO TAJNO”	TOP SECRET
„Titkos!”	“TAJNO”	SECRET
„Bizalmas!”	“POVJERLJIVO”	CONFIDENTIAL
„Korlátozott terjesztésű!”	“INTERNO”	RESTRICTED

5. CIKK

MINŐSÍTETT ADATHOZ VALÓ HOZZÁFÉRÉS

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

6. CIKK

BIZTONSÁGI ALAPELVEK

(1) Az átadó fél:
a) biztosítja, hogy a minősített adaton a nemzeti jogszabályok és egyéb szabályok rendelkezéseinek megfelelő minősítési szint feltüntetésre kerüljön;
b) tájékoztatja az átvevő felet a minősített adat felhasználásával kapcsolatos esetleges feltételekről;
c) haladéktalanul, írásban tájékoztatja az átvevő felet az adat minősítésében vagy a minősítés érvényességi idejében bekövetkezett későbbi változásokról.

(2) Az átvevő fél:
a) biztosítja, hogy a minősített adaton feltüntetésre kerüljön a jelen Egyezmény 4. Cikke alapján meghatározott egyenértékű minősítési szint;
b) ugyanolyan szintű védelemben részesíti a minősített adatot, mint amelyet a saját, azonos minősítési szintű nemzeti minősített adata számára biztosít;
c) mindaddig biztosítja a minősített adat minősítési szintjének megfelelő védelmet, amíg az átadó féltől a minősített adat minősítésének megszüntetéséről vagy minősítési szintjének vagy érvényességi idejének megváltoztatásáról írásban tájékoztatást nem kap;
d) biztosítja, hogy az átadó fél előzetes írásbeli hozzájárulása nélkül a minősített adatot harmadik fél részére nem adja át;
e) a minősített adatot kizárólag az átadás során megjelölt célra használja fel, betartva az átadó fél által a felhasználással kapcsolatban meghatározott feltételeket.

7. CIKK

BIZTONSÁGI EGYÜTTMŰKÖDÉS

(1) Az összeegyeztethető szintű biztonsági követelmények fenntartása érdekében a nemzeti biztonsági hatóságok tájékoztatják egymást a minősített adat védelmével kapcsolatos nemzeti jogszabályaikról és egyéb szabályaikról, valamint mindezek gyakorlati alkalmazásáról.

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

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

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

5) Jelen Egyezmény alapján megvalósuló együttműködés angol nyelven történik.

8. CIKK

MINŐSÍTETT SZERZŐDÉSEK

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

(2) A nemzeti biztonsági hatóság kérheti a másik Fél nemzeti biztonsági hatóságától biztonsági ellenőrzés lefolytatását a másik Fél országának 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 minősített szerződés valamennyi elemének minősítési szintjével kapcsolatos rendelkezéseket határozza meg. A projekt biztonsági utasítás másolatát azon Fél nemzeti biztonsági hatósága részére kell továbbítani, amelynek joghatósága alatt a minősített szerződés teljesítése történik.

9. CIKK

A MINŐSÍTETT ADAT TOVÁBBÍTÁSA

(1) A minősített adat továbbítása az átadó fél nemzeti jogszabályainak és egyéb szabályainak rendelkezésivel összhangban, diplomáciai úton történik.
(2) A Felek, a nemzeti biztonsági hatóságok által írásban jóváhagyott eljárási rend szerint, elektronikus úton is továbbíthatnak minősített adatot.

10. CIKK

A MINŐSÍTETT ADAT SOKSZOROSÍTÁSA, KIVONATOLÁSA, FORDÍTÁSA ÉS MEGSEMMISÍTÉSE

(1) Jelen Egyezmény alapján átadott minősített adatról készült másolatokon, kivonatokon 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 fel kell tüntetni a fordítás nyelvén azt, hogy az átadó fél minősített adatát tartalmazza.

(3) Jelen Egyezmény alapján átadott „Szigorúan titkos!”/ “STROGO TAJNO”/ TOP SECRET minősítésű adat csak az átadó fél előzetes, írásbeli engedélyével sokszorosítható, kivonatolható vagy fordítható.

(4) A minősített adatot olyan válsághelyzet esetén, amely lehetetlenné teszi a minősített adat védelmét, vagy az átadó félhez való visszajuttatását, haladéktalanul meg kell semmisíteni. A minősített adat megsemmisítéséről az átvevő fél nemzeti biztonsági hatósága az átadó fél nemzeti biztonsági hatóságát írásban értesíti.

11. CIKK

LÁTOGATÁSOK

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

(2) A látogatást kezdeményező Fél nemzeti biztonsági hatósága látogatási kérelem formájában legalább húsz nappal a látogatás kezdő időpontja előtt értesíti a fogadó Fél nemzeti biztonsági

hatóságát a tervezett látogatásról. Sürgős esetben, a nemzeti biztonsági hatóságok közötti előzetes egyeztetést követően a látogatási kérelem a látogatás kezdetéhez közelebbi időpontban is benyújtható.

(3) A látogatási kérelem az alábbiakat tartalmazza:

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

b) a látogató beosztásának és a látogató által képviselt jogi személy vagy egyéb szervezeti egység megjelölése;

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

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

e) a látogatás célja, beleértve a látogatással érintett legmagasabb minősítési szintű minősített adat minősítési szintjének megjelölését;

f) a meglátogatandó minősített adatokat kezelő szerv neve és címe, valamint a kapcsolattartójának neve, telefonszáma, fax száma, e-mail címe;

g) dátum, aláírás és a nemzeti biztonsági hatóság hivatalos pecsétjének lenyomata.

(4) A nemzeti biztonsági hatóságok közösen meghatározhatják a visszatérő látogatásra jogosult személyek listáját. A visszatérő látogatók listájának nemzeti biztonsági hatóságok által való elfogadása után a látogatások időpontjairól a látogató és fogadó fél közvetlenül állapodik meg.

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

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

12. CIKK

A MINŐSÍTETT ADAT BIZTONSÁGÁNAK MEGSÉRTÉSE

(1) A nemzeti biztonsági hatóságok haladéktalanul, írásban tájékoztatják egymást a minősített adat biztonságának megsértéséről vagy annak gyanújáról.

(2) Azon Fél nemzeti biztonsági hatósága, ahol a minősített adat biztonságának megsértésére sor került, haladéktalanul intézkedik a minősített adat biztonsága megsértésének kivizsgálása iránt.

(3) Az átvevő fél nemzeti biztonsági hatósága minden esetben írásban tájékoztatja az átadó fél nemzeti biztonsági hatóságát a minősített adat biztonságának megsértésével kapcsolatos körülményekről, a valószínűsített 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 Feleknek az Egyezmény hatálybalépéshez szükséges nemzeti jogi feltételek teljesítésére vonatkozó, diplomáciai úton küldött utolsó értesítése kézhezvételének napját követő második hónap első napján lép hatályba.

(2) Jelen Egyezmény a Felek kölcsönös egyetértésével írásban módosítható.

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

(4) Jelen Egyezmény megszűnésétől függetlenül az annak alapján kicserélt vagy keletkezett valamennyi minősített adatot az Egyezményben meghatározott rendelkezések szerint kell védelemben részesíteni, mindaddig, amíg az átadó fél írásban felmentést nem ad az átvevő fél részére ezen kötelezettség alól.

(5) Felek a jelen Egyezmény értelmezéséből vagy végrehajtásából fakadó vitákat a Felek közötti egyeztetés és tárgyalás útján, külső igazságszolgáltatási fórum igénybevétele nélkül kötelesek rendezni.

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

Készült Budapesten, 2016. október 6-án, két eredeti példányban magyar, montenegrói és angol nyelven, valamennyi szöveg egyaránt hiteles. Eltérő értelmezés esetén az angol nyelvű szöveg az irányadó.

MAGYARORSZÁG KORMÁNYA RÉSZÉRŐL	**MONTENEGRÓ KORMÁNYA RÉSZÉRŐL”**

„AGREEMENT BETWEEN THE GOVERNMENT OF HUNGARY AND THE GOVERNMENT OF MONTENEGRO ON THE EXCHANGE AND MUTUAL PROTECTION OF CLASSIFIED INFORMATION

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

Recognising the importance of mutual cooperation between the Parties,

Realising that good cooperation may require exchange of classified information between the Parties,

Recognising that they ensure equivalent protection for the classified information,

Wishing to ensure the protection of classified information exchanged between them or between the legal entities 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

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.

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 to the national laws and regulations of the Parties, the result of which may lead to unauthorised disclosure, loss, destruction, misappropriation, access or any other type of compromise of classified information;

b) **"classified contract"** means a contract that involves or requires access to classified information;

c) **"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;

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) **facility security clearance**" means the determination by a national security authority that a legal entity, possessing the legal capacity, has the physical and organizational capability to handle and store classified information in accordance with the national laws and regulations;

f) "**national security authority**" means the state authority responsible for the application and supervision of this Agreement;

g) **"need-to-know**" means the principle, according to which access to 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;

h) **"originating party"** means the Party including the legal entities, other organisational units or individuals under its jurisdiction, which releases classified information;

i) "**personnel security clearance**" means the determination by a national security authority that an individual is eligible to have access to classified information in accordance with the national laws and regulations;

j) **"recipient party"** means the Party including the legal entities, other organisational units or individuals under its jurisdiction, which receives classified information;

k) **"sub-contract"** means a contract entered into by a contractor with another contractor (the sub-contractor) for a provision of goods or services.;
l) **"sub-contractor"** means an individual or a legal entity to whom a contractor lets a sub-contract;

m) **"third party"** means any state including the legal entities, other organisational units or individuals under its jurisdiction or international organisation not being a party to this Agreement.

ARTICLE 3
NATIONAL SECURITY AUTHORITIES

(1) The national security authorities of the Parties are:

In Hungary:
Nemzeti Biztonsági Felügyelet (National Security Authority)

In Montenegro:
Directorate for protection of classified information (National Security Authority)
Direkcija za zaštitu tajnih podataka

(2) The national security authorities shall provide each other with official contact details and shall inform each other of any subsequent changes regarding to the national security authorities.

ARTICLE 4
SECURITY CLASSIFICATION LEVELS AND MARKINGS

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

In Hungary	In Montenegro	Equivalent in English language
„Szigorúan titkos!"	"STROGO TAJNO"	TOP SECRET
„Titkos!"	"TAJNO"	SECRET

„Bizalmas!”	“POVJERLJIVO”	CONFIDENTIAL
„Korlátozott terjesztésű!”	“INTERNO”	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 in writing without undue delay of any subsequent changes in the security classification level or duration of classification.

(2) The recipient party shall:
a) ensure that classified information is marked with equivalent security classification 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 protection to the classified information equivalent to its classification level until the written notification from the originating party about the declassification or the change of the security classification level or validity of the classified information;
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 national security authorities shall 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 and facility security clearance issued by the other Party. Article 4 of this Agreement shall apply accordingly.

(4) The national security authorities shall promptly notify each other about changes in the recognised personnel security clearance and facility security clearance, 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/sub-contractors as well as individuals participating in pre-contractual negotiations or in the implementation of classified contracts have appropriate personnel security clearance or facility security clearance.

(2) The national security authority may request 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 OR TRANSMISSION OF CLASSIFIED INFORMATION

(1) Classified information shall be transferred in accordance with the national laws and regulations of the originating party through diplomatic channels.

(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, EXTRACTION, TRANSLATION AND DESTRUCTION OF CLASSIFIED INFORMATION

(1) Reproductions, extractions 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!”/ “STROGO TAJNO”/TOP SECRET shall be reproduced, extracted or translated only upon the prior written consent of the originating party.

(4) In case of a crisis situation in which it is impossible to protect or to return the classified information to the originating party the classified information 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 or other organisational units represented;
c) visitor’s personnel security clearance level and its validity;
d) date and duration of the visit, and in case of recurring visits the total period of time covered by the visits;
e) purpose of the visit including the highest security classification level of classified information involved;
f) name and address of the facility to be visited, as well as the name, phone/fax number, e-mail address of its point of contact;
g) date, signature and stamping of the official seal of the national security authority.

(4)The national security authorities may agree on a list of visitors entitled to recurring visits. Once such lists have been approved by the national security authorities, the dates of the visits shall be arranged directly between the visiting and hosting entities.

(5) Classified information acquired by a visitor shall be considered as classified information received under this Agreement.

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

ARTICLE 12
BREACH OF SECURITY

(1) The national security authorities shall without undue delay inform each other in writing of any breach of security or suspicion thereof.

(2) The national security authority of the party where the breach of security has occurred, shall investigate the incident without undue delay.

(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 possible 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.

(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 6th October 2016 in two originals, in Hungarian, Montenegrin 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 Montenegro”

4. §

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

(2) A 2. § és a 3. § az Egyezmény 14. cikk (1) bekezdésében meghatározott időpontban lép hatályba.

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

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

Indokolás a Magyarország Kormánya és Montenegró 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, az Olasz Köztársasággal és a Német Szövetségi Köztársasággal kötött általános titokvédelmi egyezményt, amelyek alkalmazását a 2010. március 31-ig hatályos, az államtitokról és szolgálati titokról szóló 1995. évi LXV. törvény nem tette lehetővé.

A Mavtv. 2010. április 1-jei hatálybalépésével azonban megteremtette a kétoldalú titokvédelmi megállapodások megkötéséhez és alkalmazásához szükséges jogi alapokat, és így megkezdődhetett hazánk e téren tapasztalható elmaradásának felszámolása.

Ennek megfelelően hazánk a 46/2011. (VI. 21.) ME határozat értelmében először a Szlovák Köztársasággal, a Lengyel Köztársasággal és a Cseh Köztársasággal kezdte meg a tárgyalásokat, amelyek eredményeképpen 2012. május 3-án aláírásra került Budapesten a Szlovák Köztársaság és Magyarország, 2012. június 13-án a Cseh Köztársaság és Magyarország, 2014. január 29-én a Lengyel Köztársaság és Magyarország közötti megállapodás. Továbbá az 58/2012. (V. 16.) ME határozat alapján 2012. augusztus 29-én a Lett Köztársaság és Magyarország, 2012. december 11-én a Francia Köztársaság és Magyarország, 2013. március 22-én az Osztrák Köztársaság és Magyarország között hasonló megállapodást, valamint az 54/2013. ME határozat alapján 2014. július 3-án a Macedón Köztársaság és Magyarország, 2014. szeptember 8-án az Albán Köztársaság és Magyarország között jött létre a minősített adatok cseréjéről és kölcsönös védelméről szóló egyezmény. Az 58/2012. (V. 16.) ME határozat alapján létrehozásra került a Belga Királyság és Magyarország közötti megállapodás, amelynek aláírására 2015. szeptember 21-én került sor, az 54/2013. (IV. 16.) ME határozat alapján pedig a Ciprusi Köztársaság és Magyarország közötti megállapodás jött létre, amelynek aláírására 2015. október 29-én került sor. 2015. november 25-én aláírásra került az 58/2012. (V. 16.) ME határozat alapján létrehozott megállapodás Magyarország és az Olasz Köztársaság között. Az 54/2013. (IV. 10.) ME határozat alapján 2016-ban négy megállapodás aláírására került sor; 2016. január 22-én a Szlovén Köztársasággal, 2016. június 10-én a Horvát Köztársasággal, 2016. június 15-én Spanyolországgal.

2016. október 6-án, Budapesten sor került *a Magyarország Kormánya és Montenegró Kormánya között a minősített adatok cseréjéről és kölcsönös védelméről szóló egyezmény* (a továbbiakban: Egyezmény) aláírására, amelyre *a Magyarország Kormánya és Montenegró Kormánya között a*

minősített adatok cseréjéről és kölcsönös védelméről szóló egyezmény szövegének végleges megállapítására adott felhatalmazásról szóló 1309/2016. (VI. 13.) Korm. határozat adott felhatalmazást.

A Mavtv.-ben foglaltak végrehajtása, Magyarország nemzetközi kötelezettségvállalásainak teljesítése, továbbá a minősített adatok cseréjével és kölcsönös védelmével történő szorosabb együttműködés biztosítása miatt azonban indokolt új szerződések megkötése.

RÉSZLETES INDOKOLÁS

az 1. §-hoz

A Javaslat 1. §-a a nemzetközi szerződésekkel kapcsolatos eljárásról szóló 2005. évi L. törvény 7. § (1)-(3) bekezdésének, valamint 10. § (1) bekezdés *a)* pontjának megfelelően tartalmazza az Egyezmény kötelező hatályának elismerésére adott országgyűlési felhatalmazást.

a 2. és 3. §-hoz

A Javaslat 2. §-a és 3. §-a a nemzetközi szerződésekkel kapcsolatos eljárásról szóló 2005. évi L. törvény 10. § (1) bekezdés *b)* pontjának megfelelően rendelkezik az Egyezmény kihirdetéséről, és tartalmazza az Egyezmény magyar és angol nyelvű hiteles szövegét.

Az Egyezmény célja, hogy védelmet biztosítson a Szerződő Felek, valamint a joghatóságuk alá tartozó állami szervek, illetve egyéb, például gazdasági szervezetek közötti együttműködés során kicserélt vagy keletkezett minősített adatok számára. Ennek keretében szabályozza a Felek közötti biztonsági együttműködést, kijelöli a hatáskörrel rendelkező hatóságokat, és rendelkezik egyes nemzeti minősítési szintek egymásnak történő megfeleltethetőségéről, valamint a minősített adat biztonságának megsértése esetén alkalmazandó eljárásról.

a 4. §-hoz

A Javaslat – a 2. és 3. § kivételével – a kihirdetését követő napon lép hatályba. A 2. § és 3. § hatálybalépése az Egyezmény hatálybalépéséhez igazodik. Az Egyezmény „a Felek által az Egyezmény hatálybalépéshez szükséges belső eljárások lefolytatásáról szóló, diplomáciai úton küldött utolsó írásbeli értesítés kézhezvételének napját követő második hónap első napján lép hatályba.” Ennek oka, hogy az Egyezmény kötelező hatályának elismerésére a Felek által alkalmazandó alkotmányos vagy belső jogi szabályokkal és eljárásokkal összhangban kerül sor. Az Egyezmény hatálybalépésének naptári napját a külpolitikáért felelős miniszter annak ismertté válását követően a Magyar Közlönyben közzétett egyedi közleményével állapítja meg.