Miniszterelnökség

Iromány száma: **T/3519.**

Benyújtás dátuma: **2023-04-04 23:14**

Parlex azonosító: **1K5AXVFO0001**

Címzett: **Kövér László, az Országgyűlés elnöke**
Tárgy: **Törvényjavaslat benyújtása**
Benyújtó: **Dr. Semjén Zsolt, miniszterelnök-helyettes**
Előadó: **Rogán Antal, Miniszterelnöki Kabinetirodát vezető miniszter**

Törvényjavaslat címe: **A Magyarország Kormánya és Bosznia-Hercegovina Minisztertanácsa között a minősített adatok cseréjéről és kölcsönös védelméről szóló egyezmény kihirdetéséről**

A Kormány nevében benyújtom a Magyarország Kormánya és Bosznia-Hercegovina Minisztertanácsa között a minősített adatok cseréjéről és kölcsönös védelméről szóló egyezmény kihirdetéséről szóló törvényjavaslatot.

2023. évi ..... törvény

a Magyarország Kormánya és Bosznia-Hercegovina Minisztertanácsa között a minősített adatok cseréjéről és kölcsönös védelméről szóló egyezmény kihirdetéséről

1. §

Az Országgyűlés e törvénnyel felhatalmazást ad a Magyarország Kormánya és Bosznia-Hercegovina 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. §

(1) Az Egyezmény hiteles magyar nyelvű szövegét az 1. melléklet tartalmazza.

(2) Az Egyezmény hiteles angol nyelvű szövegét a 2. melléklet tartalmazza.

4. §

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

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

(3) Az Egyezmény, a 2. §, a 3. §, valamint az 1. melléklet és a 2. melléklet hatálybalépésének naptári napját a külpolitikáért felelős miniszter annak ismertté válását követően a Magyar Közlönyben haladéktalanul közzétett közleményével állapítja meg.

5. §

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

1. melléklet a 2023. évi ..... törvényhez

EGYEZMÉNY MAGYARORSZÁG KORMÁNYA ÉS BOSZNIA-HERCEGOVINA MINISZTERTANÁCSA KÖZÖTT A MINŐSÍTETT ADATOK CSERÉJÉRŐL ÉS KÖLCSÖNÖS VÉDELMÉRŐL

Magyarország Kormánya és Bosznia-Hercegovina Minisztertanácsa (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 Magyarország és Bosznia-Hercegovina érdekeit és biztonságát, az alábbiakban állapodtak meg:

1. CIKK

FOGALOM-MEGHATÁROZÁSOK

Jelen Egyezmény alkalmazásában:

a) minősített adat: megjelenési formájától, természetétől függetlenül minden olyan adat, amelyet bármelyik Fél jogszabályai és egyéb szabályai szerint védelemben kell részesíteni a minősített adat biztonságának megsértésével szemben, és amelyet ennek megfelelően minősítettek;

b) a minősített adat biztonságának megsértése: olyan tett vagy mulasztás, amely jelen Egyezménnyel vagy a Felek jogszabályaival és egyéb szabályaival ellentétes, és amely a minősített adat jogosulatlan nyilvánosságra hozatalát, elvesztését, megsemmisülését, jogosulatlan felhasználását, megszerzését vagy egyéb módon történő megsértését eredményezheti;

c) nemzeti biztonsági hatóság: az állami szerv, amely jelen Egyezmény végrehajtásáért és felügyeletéért felelős;

d) átadó fél: az a fél – beleértve a joghatósága alá tartozó jogi személyeket vagy természetes személyeket –, amelyik a minősített adatot átadja;

e) átvevő fél: az a fél – beleértve a joghatósága alá tartozó jogi személyeket vagy természetes személyeket –, amelyik a minősített adatot átveszi;

f) harmadik fél: bármely olyan állam – beleértve a joghatósága alá tartozó jogi személyeket és természetes személyeket- vagy nemzetközi szervezet, amely nem részese jelen Egyezménynek;

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) személyi biztonsági tanúsítvány: a nemzeti biztonsági hatóság azon döntése, amely megállapítja, hogy egy személy a Felek jogszabályaival és egyéb szabályaival összhangban hozzáférhet minősített adatokhoz;

i) telephely biztonsági tanúsítvány: a nemzeti biztonsági hatóság azon döntése, amely szerint a jogképességgel rendelkező jogi személy vagy természetes személy a Felek jogszabályaival és egyéb szabályaival összhangban rendelkezik a minősített adatok kezelésére és tárolására való fizikai és szervezeti képességgel;

j) minősített szerződés: az egyik fél jogi személye vagy természetes személye és a másik fél jogi személye vagy természetes személye között kötött olyan szerződés vagy alvállalkozói szerződés, amelynek végrehajtása vagy megkötése esetén minősített adathoz való hozzáférésre van szükség;

k) szerződő: olyan jogi személy vagy természetes személy, aki a Felek jogszabályaival és szabályaival összhangban rendelkezik a minősített szerződések megkötésére irányuló képességgel;

l) projekt biztonsági utasítás (PSI): azon biztonsági szabályok/ eljárások összessége, melyeket egy meghatározott projekt esetén alkalmazni kell.

2. CIKK

NEMZETI BIZTONSÁGI HATÓSÁGOK

(1) A Felek nemzeti biztonsági hatóságai:

Magyarországon: Nemzeti Biztonsági Felügyelet,

Bosznia-Hercegovinában: Ministarstvo sigurnosti, Sektor za zaštitu tajnih podataka – Državni sigurnosni organ (Biztonságért felelős Minisztérium, Minősített Adatvédelmi Részleg – Nemzeti Biztonsági Felügyelet).

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

(3) A nemzeti biztonsági hatóságok nevében bekövetkező változások nem tekintendőek ezen Egyezmény módosításának. A nemzeti biztonsági hatóságok írásban tájékoztatják egymást e változásokról.

3. CIKK

MINŐSÍTÉSI SZINTEK ÉS JELÖLÉSEK

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

Magyarországon	Bosznia-Hercegovinában	Angol nyelvű megfelelőjük
„Szigorúan titkos!”	VRLO TAJNO	TOP SECRET
„Titkos!”	TAJNO	SECRET
„Bizalmas!”	POVJERLJIVO	CONFIDENTIAL
„Korlátozott terjesztésű!”	INTERNO	RESTRICTED

4. CIKK

MINŐSÍTETT ADATHOZ VALÓ HOZZÁFÉRÉS

Jelen Egyezmény alapján minősített adathoz kizárólag olyan természetes személyek kaphatnak hozzáférést, akik a szükséges ismeret elvének megfelelnek, és az érintett fél vonatkozó jogszabályaival és egyéb szabályaival összhangban megfelelően felhatalmazást kaptak a minősített adathoz való hozzáférésre.

5. CIKK

BIZTONSÁGI ALAPELVEK

(1) Az átadó fél:

a) biztosítja, hogy a minősített adaton a jogszabályainak és egyéb szabályainak 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 érvényességi idejében bekövetkezett változásokról.

(2) Az átvevő fél:

a) biztosítja, hogy a minősített adaton feltüntetésre kerüljön jelen Egyezmény 3. cikke alapján meghatározott egyenértékű minősítési szint;

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

c) mindaddig biztosítja a minősített adat minősítési szintjének megfelelő védelmet, amíg az átadó féltől az átvett 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 az átvett minősített adatot harmadik fél részére nem adja át;

e) a minősített adatot kizárólag az átadás során megjelölt célra használja fel, betartva az átadó fél által meghatározott esetleges feltételeket.

6. CIKK

BIZTONSÁGI EGYÜTTMŰKÖDÉS

(1) A nemzeti biztonsági hatóságok megkeresésre tájékoztatják egymást a minősített adatok védelmével kapcsolatos jogszabályaikról és egyéb szabályaikról, valamint mindezek gyakorlati alkalmazásáról.

(2) Megkeresés esetén a Felek, összhangban jogszabályaikkal és egyéb szabályaikkal, segítséget nyújtanak egymásnak a személyi biztonsági tanúsítványokkal és a telephely biztonsági tanúsítványokkal kapcsolatos eljárások során. A Felek nemzeti biztonsági hatóságai megállapodnak a segítségnyújtás folyamatáról és mértékéről, ideértve a biztonsági ellenőrzés lefolytatásához szükséges minimális információkat is.

(3) A Felek megkeresés esetén jogszabályaikkal és egyéb szabályaikkal összhangban elismerik a másik fél által kibocsátott személyi biztonsági tanúsítványokat és telephely biztonsági

tanúsítványokat. Mindezek során a jelen Egyezmény 3. Cikkében foglaltak alkalmazandók.

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

(5) A jelen Egyezmény alapján megvalósuló együttműködés angol nyelven történik.

7. CIKK

MINŐSÍTETT SZERZŐDÉSEK

(1) A minősített szerződéseket a Felek jogszabályai és egyéb szabályai alapján kell megkötni és teljesíteni. A nemzeti biztonsági hatóságok megkeresésre megerősítik, hogy a lehetséges szerződők és a szerződéskötést megelőző tárgyalásokban vagy a minősített szerződések teljesítésében részt vevők rendelkeznek megfelelő személyi biztonsági tanúsítvánnyal vagy telephely biztonsági tanúsítvánnyal.

(2) Az egyik fél nemzeti biztonsági hatósága megkeresésre, a területén lévő létesítményről, különösen annak minősített adatot kezelő képességéről tájékoztatást ad a másik fél nemzeti biztonsági hatóságának.

(3) A minősített szerződések kötelező részét képezi a projekt biztonsági utasítás, amely a biztonsági követelményeket és a szerződés egyes elemeinek minősítésével kapcsolatos rendelkezéseket határozza meg. A projekt biztonsági utasítás másolatát azon fél nemzeti biztonsági hatósága részére kell továbbítani, amelynek joghatósága alatt a minősített szerződés végrehajtása történik.

8. CIKK

A MINŐSÍTETT ADAT TOVÁBBÍTÁSA

(1) A minősített adat továbbítása az átadó fél jogszabályai és egyéb szabályai szerint, diplomáciai úton, vagy a nemzeti biztonsági hatóságok által írásban közösen meghatározott egyéb módon történik.

(2) A Felek a nemzeti biztonsági hatóságok által írásban jóváhagyott biztonsági eljárási rend szerint, elektronikus úton is továbbíthatnak minősített adatot.

9. CIKK

A MINŐSÍTETT ADAT SOKSZOROSÍTÁSA, KIVONATOLÁSA, FORDÍTÁSA ÉS MEGSEMMISÍTÉSE

(1) A minősített adat másolását, kivonatolását, fordítását és megsemmisítését az átadó fél korlátozhatja vagy kizárhatja.

(2) A 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 minimumra kell korlátozni.

(3) A jelen Egyezmény alapján átadott minősített adatról készült fordításokon a fordítás nyelvén fel kell tüntetni, hogy az az átadó fél minősített adatát tartalmazza.

(4) A jelen Egyezmény alapján átadott „Szigorúan titkos!”/ VRLO TAJNO / TOP SECRET minősítésű adat sokszorosítása, kivonatolása vagy fordítása kizárólag az átadó fél előzetes írásbeli hozzájárulásával történhet.

(5) A jelen Egyezmény alapján átadott „Szigorúan titkos!”/ VRLO TAJNO / TOP SECRET minősítésű adat nem semmisíthető meg és az átadó fél részére kell visszaküldeni.

(6) Olyan válsághelyzet esetén, amely lehetetlenné teszi a minősített adat védelmét vagy visszajuttatását az átadó félnek, a minősített adatot haladéktalanul meg kell semmisíteni. A minősített adat megsemmisítésről az átvevő fél nemzeti biztonsági hatósága haladéktalanul, írásban értesíti az átadó fél nemzeti biztonsági hatóságát.

10. CIKK

LÁTOGATÁSOK

(1) Minősített adathoz való hozzáférést igénylő látogatásra a fogadó fél nemzeti biztonsági hatóságának előzetes írásbeli hozzájárulása alapján kerülhet sor.

(2) A látogatást kezdeményező fél nemzeti biztonsági hatósága a tervezett látogatásról a fogadó fél nemzeti biztonsági hatóságának legalább húsz nappal a látogatás időpontja előtt látogatási kérelmet küld. Sürgős esetben a nemzeti biztonsági hatóságok előzetes egyeztetését követően a látogatási kérelem a látogatás kezdetéhez közelebbi időpontban is benyújtható.

(3) A látogatási kérelemnek 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 intézménynek a 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 szintjét;

f) a meglátogatandó létesítmény 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 látogatások további részleteit a nemzeti biztonsági hatóságok állapítják meg.

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

(6) A Felek jogszabályaikkal és egyéb szabályaikkal összhangban biztosítják a látogatók személyes adatainak védelemét.

11. CIKK

A MINŐSÍTETT ADAT BIZTONSÁGÁNAK MEGSÉRTÉSE

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

(2) Annak a félnek a nemzeti biztonsági hatósága, ahol a minősített adat biztonságának megsértése bekövetkezett, köteles haladéktalanul kezdeményezni az esemény kivizsgálását. A másik fél nemzeti biztonsági hatósága szükség esetén közreműködik a vizsgálatban.

(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 kár mértékéről, a kár enyhítése érdekében megtett intézkedésekről, valamint a vizsgálat eredményéről.

12. CIKK

KÖLTSÉGEK VISELÉSE

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

13. CIKK

MÁS NEMZETKÖZI EGYEZMÉNYEKHEZ VALÓ VISZONY

Jelen Egyezmény nem érinti a Felek egyéb két- vagy többoldalú egyezmény alapján fennálló kötelezettségeit, ideértve mindazon megállapodásokat és egyetértési megállapodásokat, amelyek minősített adatok cseréjét és kölcsönös védelmét szabályozzák.

14. CIKK

ZÁRÓ RENDELKEZÉSEK

(1) Jelen Egyezmény határozatlan időre jön létre. Jelen Egyezmény a Felek által az Egyezmény hatálybalépéséhez szükséges belső jogi feltételek teljesítésére vonatkozó, diplomáciai úton küldött utolsó írásbeli értesítés kézhezvételének napját követő második hónap első napján lép hatályba.

(2) Jelen Egyezmény a Felek kölcsönös egyetértésével írásban módosítható. A módosítások hatálybalépésével kapcsolatban a jelen cikk (1) bekezdésében foglaltak az irányadók.

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

(4) Az Egyezmény megszűnésétől függetlenül az annak alapján átadott vagy keletkezett 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) Jelen Egyezmény végrehajtásából vagy értelmezéséből fakadó vitákat a Felek egymás közötti egyeztetés vagy tárgyalás útján, diplomáciai úton rendezik.

Fentiek tanúbizonyságául, az alulírott és az erre felhatalmazott megbízottak jelen Egyezményt

aláírásukkal látták el.

Készült Bécsben, 2021.10.19-én, két eredeti példányban, magyarul, Bosznia-Hercegovina hivatalos nyelvein (bosnyákul, horvátul és szerbül) és angol nyelven, valamennyi szöveg egyaránt hiteles.

Eltérő értelmezés esetén az angol nyelvű szöveg az irányadó.

AGREEMENT BETWEEN THE GOVERNMENT OF HUNGARY AND THE COUNCIL OF MINISTERS OF BOSNIA AND HERZEGOVINA ON THE EXCHANGE AND MUTUAL PROTECTION OF CLASSIFIED INFORMATION

The Government of Hungary and the Council of Ministers of Bosnia and Herzegovina (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 the interests and security of Hungary and Bosnia and Herzegovina, agreed upon the following:

ARTICLE 1

DEFINITIONS

For the purpose of this Agreement:

a) ’classified information’ means any information that, regardless of its form or nature, under the laws and regulations of either Party, requires protection against breach of security and has been duly designated;

b) ’breach of security’ means an act or an omission which is contrary to this Agreement or to the 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;

c) ’national security authority’ means the state authority responsible for the application and supervision of this Agreement;

d) ’originating party’ means the Party including the legal entities or individuals under its jurisdiction, which releases classified information;

e) ’recipient party’ means the Party including the legal entities or individuals under its jurisdiction, which receives classified information;

f)’third party’ means any state including the legal entities or individuals under its jurisdiction or international organisation not being a party to 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) ’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 laws and regulations of the Parties;

i) ’facility security clearance’ means the determination by a national security authority that a legal entity or an individual, possessing the legal capacity, has the physical and organizational capability to handle and store classified information in accordance with the laws and regulations of the Parties;

j) ’classified contract’ means a contract or a sub-contract between the legal entity or individual of one party and the legal entity or individual of the other party, the implementation of which or its generation requires access to classified information;

k) ’contractor’ means a legal entity or an individual possessing the legal capacity to conclude classified contracts in accordance with the laws and regulations of the Parties;

l) ’project security instruction (PSI)’ means a compilation of security regulations/ procedures which are applied to a specific project.

ARTICLE 2

NATIONAL SECURITY AUTHORITIES

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

In Hungary: Nemzeti Biztonsági Felügyelet (National Security Authority),

In Bosnia and Herzegovina: Ministarstvo sigurnosti, Sektor za zaštitu tajnih podataka – Državni sigurnosni organ, Ministry of Security, Sector for Protection of Classified Information - National Security Authority).

(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.

(3) Changes in the names of the national security authorities shall not constitute modification of this Agreement. The national security authorities shall inform each other in writing about such changes.

ARTICLE 3

CLASSIFICATION LEVELS AND MARKINGS

The equivalence of classification levels and markings is as follows:

In Hungary	**In Bosnia and Herzegovina**	**Equivalent in English language**
„Szigorúan titkos!”	VRLO TAJNO	TOP SECRET
„Titkos!”	TAJNO	SECRET
„Bizalmas!”	POVJERLJIVO	CONFIDENTIAL
„Korlátozott terjesztésű!”	INTERNO	RESTRICTED

ARTICLE 4

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 laws and regulations of the respective Party.

ARTICLE 5

SECURITY PRINCIPLES

(1) The originating party shall:

a) ensure that classified information is marked with appropriate classification markings in accordance with its laws and regulations;

b) inform the recipient party of any restrictions of usage of classified information;

c) inform the recipient party in writing without undue delay of any subsequent changes in the classification level or duration of classification.

(2) The recipient party shall:

a) ensure that classified information is marked with equivalent classification marking in accordance with Article 3 of this Agreement;

b) afford the same degree of protection to classified information as afforded to its own classified information of equivalent classification level;

c) ensure protection of the classified information equivalent to its classification level until the written notification from the originating party about the declassification or the change of the 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 any restriction given by the originating party.

ARTICLE 6

SECURITY CO-OPERATION

(1) The national security authorities shall, on request, inform each other of their laws and regulations concerning protection of classified information and the practices stemming from their implementation.

(2) On request, the Parties shall, in accordance with their laws and regulations, assist each other during the personnel security clearance procedures and facility security clearance procedures. The national security authorities of the Parties shall agree on the procedures and standards of the assistance including the minimum information to fulfill the security vetting procedure.

(3) On request, the Parties shall in accordance with their laws and regulations, recognise the personnel security clearances and facility security clearances issued by the other Party. Article 3 of this Agreement shall apply accordingly.

(4) The national security authorities shall promptly notify each other about changes in the

recognised personnel security clearances and facility security clearances, especially in case of their withdrawal.

(5) The co-operation under this Agreement shall be effected in the English language.

ARTICLE 7

CLASSIFIED CONTRACTS

(1) Classified contracts shall be concluded and implemented in accordance with the laws and regulations of each Party. On request, the national security authorities shall confirm that proposed contractors as well as individuals participating in pre-contractual negotiations or in the implementation of classified contracts have appropriate personnel security clearance or facility security clearance.

(2) On request, the national security authority of one Party shall provide information to the national security authority of the other Party about the facility located in the territory of the one Party, including the capability of the facility to handle classified information.

(3) Classified contracts shall contain project security instructions on the security requirements and on the 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 8

TRANSFER OR TRANSMISSION OF CLASSIFIED INFORMATION

(1) Classified information shall be transfered in accordance with the laws and regulations of the originating party through diplomatic channels or as otherwise agreed in writing between the national security authorities.

(2) The Parties may transmit classified information by electronic means in accordance with the security procedures approved by the national security authorities in writing.

ARTICLE 9

REPRODUCTION, EXTRACTION, TRANSLATION AND DESTRUCTION OF CLASSIFIED INFORMATION

(1) The reproduction, extraction, translation and destruction of classified information may be restricted or excluded by the originating party.

(2) Reproductions, extractions and translations of classified information released under this Agreement shall bear appropriate classification markings and shall be protected as the originals. Number of reproductions shall be limited to that required for official purposes.

(3) 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.

(4) Classified information released under this Agreement marked „Szigorúan titkos!”/ VRLO TAJNO / TOP SECRET shall be reproduced, extracted or translated only upon the prior written consent of the originating party.

(5) Classified information released under this Agreement marked „Szigorúan titkos!”/ VRLO TAJNO / TOP SECRET shall not be destroyed and shall be returned to the originating party.

(6) In case of a crisis situation in which it is impossible to protect or to return the classified information to the originating party it shall be destroyed without undue delay. The national security authority of the recipient party shall notify the national security authority of the originating party in writing about the destruction of the classified information.

ARTICLE 10

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 organisation 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 classification level of classified information involved;

f) name and address of the facility to be visited, as well as the name, phone/fax number, e-mail address of its point of contact;

g) date, signature and stamping of the official seal of the national security authority.

(4) The national security authorities may agree on a list of visitors entitled to recurring visits. The national security authorities shall agree on the further details of the recurring visits.

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

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

ARTICLE 11

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 initiate the investigation of the incident without undue delay. The national security authority of the other Party shall, if required, co-operate in the investigation.

(3) In any case, the national security authority of the recipient party shall inform the national security authority of the originating party in writing about the circumstances of the breach of security, the extent of the damage, the measures adopted for its mitigation and the outcome of the investigation.

ARTICLE 12

EXPENSES

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

ARTICLE 13

RELATIONSHIP WITH OTHER INTERNATIONAL AGREEMENTS

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

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 internal legal requirements for this Agreement to enter into force have been fulfilled.

(2) This Agreement may be amended on the basis of the mutual agreement of the Parties in writing. Such amendments shall enter into force in accordance with Paragraph 1 of this Article.

(3) Each Party is entitled to terminate this Agreement in writing at any time. In such a case, the validity of this Agreement shall expire after six months following the day on which the other Party receives the written notice of the termination.

(4) Regardless of the termination of this Agreement, all classified information exchanged or generated under this agreement shall be protected in accordance with the provisions set forth herein until the originating party dispenses the recipient party from this obligation in writing.

(5) Any dispute regarding the interpretation or implementation of this Agreement shall be resolved by consultations and negotiations between the Parties through diplomatic channels.

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

Done in Vienna on 19 October 2021 in two originals, in Hungarian, in the official languages of Bosnia and Herzegovina (Bosnian, Croatian, Serbian) and in English language, each text being equally authentic.

In case of different interpretation the English text shall prevail.

Általános indokolás

Ezen indokolás a jogalkotásról szóló 2010. évi CXXX. törvény 18. § (3) bekezdése, valamint a Magyar Közlöny kiadásáról, valamint a jogszabály kihirdetése során történő és a közjogi szervezetszabályozó eszköz közzététele során történő megjelöléséről szóló 5/2019. (III. 13.) IM rendelet 20. § (2) bekezdés *a)* pontja alapján a Magyar Közlöny mellékleteként megjelenő Indokolások Tárában közzétételre kerül.

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 (2004. évi LXXXIX. törvény) és a Németországi Szövetségi Köztársasággal (1996. évi XXXV. törvény) 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 Magyar Köztársaság Kormánya, valamint a Szlovák Köztársaság Kormánya, a Lengyel Köztársaság Kormánya és a Cseh Köztársaság Kormánya között minősített adatok kölcsönös védelméről szóló nemzetközi szerződések előkészítéséről és létrehozásáról szóló *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.

A Magyarország Kormánya, valamint az Amerikai Egyesült Államok Kormánya, a Belga Királyság Kormánya, az Egyesült Királyság Kormánya, az Észt Köztársaság Kormánya, a Francia Köztársaság Kormánya, a Lett Köztársaság Kormánya, a Litván Köztársaság Kormánya, a Németországi Szövetségi Köztársaság Kormánya, az Olasz Köztársaság Kormánya, az Osztrák Köztársaság Kormánya, valamint a Svéd Királyság Kormánya között minősített adatok cseréjéről és kölcsönös védelméről szóló nemzetközi szerződések előkészítéséről és létrehozásáról szóló *58/2012. (V. 16.) ME határozat* [a továbbiakban: 58/2012. (V. 16.) ME határozat] alapján 2012. augusztus 29-én a Lett Köztársaság és Magyarország, 2012. december 11-én a Francia Köztársaság és Magyarország, 2013. március 22-én az Osztrák Köztársaság és Magyarország kötött hasonló megállapodást.

A Magyarország Kormánya, valamint az Albán Köztársaság Kormánya, a Bolgár Köztársaság Kormánya, Bosznia-Hercegovina Kormánya, a Ciprusi Köztársaság Kormánya, a Finn Köztársaság Kormánya, a Holland Királyság Kormánya, a Horvát Köztársaság Kormánya, Koszovó Kormánya, a Luxemburgi Nagyhercegség Kormánya, a Macedón Köztársaság Kormánya, Montenegró Kormánya, a Portugál Köztársaság Kormánya, Románia Kormánya, a Spanyol Királyság Kormánya, a Szerb Köztársaság Kormánya, valamint a Szlovén Köztársaság Kormánya között minősített adatok cseréjéről és kölcsönös védelméről szóló nemzetközi szerződések előkészítéséről és létrehozásáról szóló *54/2013. (IV. 16.) ME határozat* [a továbbiakban: 54/2013. (IV. 16.) 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. 16.) ME határozat alapján 2016-ban négy megállapodás aláírására került sor; 2016. január 22-én a Szlovén Köztársasággal, 2016. június 10-én a Horvát Köztársasággal és 2016. június 15-én Spanyolországgal, 2016. október 6-án Montenegróval. 2016-ban további két megállapodás aláírása is megvalósult; 2016. szeptember 7-én az Oroszországi Föderációval és Dániával a minősített adatok átadásáról, minősítési szintjeinek megfeleltetéséről és védelméről szóló kétoldalú nemzetközi megállapodások létrehozására adott felhatalmazásról szóló 136/2014. (XI. 26.) ME határozat alapján, 2016. december 8-án az Észt Köztársasággal az 58/2012. (V. 16.) ME határozat alapján. 2017-ben további négy egyezmény létrehozása történt meg: az

54/2013. (IV. 16.) ME határozat alapján a Bolgár Köztársasággal 2017. július 5-én aláírt egyezményé, a Finn Köztársasággal 2017. október 25-én aláírt egyezményé, illetve az 58/2012. (V. 16.) ME határozat alapján Litvániával 2017. szeptember 8-án aláírt egyezményé, valamint a Svéd Királysággal 2017. október 25-én aláírt egyezményé. Ezt követte a 2018. augusztus 23-án az 58/2012. (V. 16.) ME határozat alapján a Német Szövetségi Köztársasággal aláírt – a reláció tekintetében a korábban említett szerződést felváltó – egyezmény, az 54/2013. (IV. 16.) ME határozat alapján a Portugál Köztársasággal 2018. június 28-án aláírt egyezmény, a Luxemburgi Nagyhercegséggel 2018. szeptember 5-én aláírt egyezmény és a 2018. október 3-án Romániával aláírt egyezmény létrehozása.

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 más államokkal is.

Részletes indokolás

1. §

Az Egyezmény tárgykörére tekintettel a nemzetközi szerződésekkel kapcsolatos eljárásról szóló 2005. évi L. törvény (a továbbiakban: Nsztv.) 7. § (1) bekezdés a) pontja, illetve (3) bekezdés b) pontja alapján az Országgyűlés ad felhatalmazást az Egyezmény kötelező hatályának elismerésére. Jelen § - az Alaptörvény 1. cikk (2) bekezdés d) pontjával, illetve az Nsztv. 7. § (2) bekezdésében foglaltakkal összhangban – a szerződéskötési eljárás e belső jogi aktusát rögzíti.

2. §

Az Nsztv. által megteremtett ún. egyszerűsített dualista-transzformációs rendszernek megfelelően a kötelező hatály elismerésére adott felhatalmazás a kihirdetéssel egy aktusba olvad össze [Nszt. 7. § (2) bekezdés, illetve 9. § (1) bekezdés]. Mivel az Egyezmény tárgyából kifolyólag az Országgyűlés a cselekvő a belső jog síkján, a kihirdetés is törvényi formát ölt.

3. §, 1-2. melléklet

Az Nsztv. 10. § (1) bekezdés b) pontjában, illetve 10. § (2) bekezdésében foglaltaknak megfelelően a törvénytervezet e szakasza és a mellékletek tartalmazzák az Egyezmény hiteles magyar és angol nyelvű 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. Az Egyezmény 1-3. cikkei rögzítik az Egyezmény tárgyát, az alapvető fogalmakat, az illetékes hatóságokat, valamint megfeleltetik

egymásnak a minősítési szinteket és jelöléseiket. A 4-12. cikkek rendelkeznek az Egyezmény hatálya alá eső biztonsági együttműködési tevékenységekről, a minősített adat biztonságának megsértése esetén alkalmazandó eljárásról, valamint a költségek viseléséről. A 13. cikk az Egyezmény más nemzetközi egyezményekhez való viszonyát rendezi, míg a 14. cikk általános záró rendelkezéseket és a hatálybalépés időpontjára vonatkozó szabályokat tartalmaz.

4. §

E szakasz rendelkezik az Egyezmény belső jogi hatálybalépésének napjáról, ami az Nsztv. 10. § (3) bekezdésének megfelelően egybeesik a nemzetközi jogi hatálybalépés időpontjával. A hatálybalépés naptári napját annak ismertté válását követően a külgazdasági és külügyminiszter a Magyar Közlönyben haladéktalanul közzétett közleményével állapítja meg. A hatálybalépés naptári napját megállapító külügyminisztériumi közleményt a külgazdasági és külügyminiszter hivatalból, a szaktárca külön közbenjárása nélkül adja ki.

5. §

Ez a szakasz megállapítja, hogy a törvény végrehajtása a minősített adatok védelmének szakmai felügyeletéért felelős miniszter feladatkörébe tartozik.