MAGYARORSZÁG KORMÁNYA

T/13087. számú

törvényjavaslat

a Magyarország Kormánya és az Oroszországi Föderáció Kormánya között a minősített adatok kölcsönös védelméről szóló egyezmény kihirdetéséről

Előadó: **Dr. Pintér Sándor**
belügyminiszter

Budapest, 2016. november

2016. évi … törvény

a Magyarország Kormánya és az Oroszországi Föderáció Kormánya között a minősített adatok kölcsönös védelméről szóló egyezmény kihirdetéséről

1. §

Az Országgyűlés e törvénnyel felhatalmazást ad a Magyarország Kormánya és az Oroszországi Föderáció Kormánya között a minősített adatok 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 AZ OROSZORSZÁGI FÖDERÁCIÓ KORMÁNYA KÖZÖTT A MINŐSÍTETT ADATOK KÖLCSÖNÖS VÉDELMÉRŐL

Magyarország Kormánya és az Oroszországi Föderáció Kormánya, a továbbiakban Felek,

attól a szándéktól vezérelve, hogy védelmet biztosítsanak azon minősített adatoknak, melyek cseréje politikai, hadi, haditechnikai, gazdasági vagy más együttműködések során történik, továbbá amelyek ilyen együttműködések alkalmával keletkeztek,

figyelembe véve a minősített adatok védelmének biztosításában rejlő közös érdekeket összhangban a Felek állama törvényeinek és egyéb jogszabályainak rendelkezéseivel, a következőkben állapodtak meg:

1. Cikk

Fogalommeghatározások

Jelen Egyezményben használt fogalmak jelentése a következő:

a) „minősítési szint jelölése”: az a jelölés, melyet közvetlenül a minősített adat hordozóján és/vagy az azt kísérő dokumentáción tüntetnek fel, meghatározva a hordozó által tartalmazott adat minősítési szintjét;

b) „biztonsági tanúsítvány”: valamely Fél állama törvényeinek és egyéb jogszabályainak rendelkezései szerint kialakított eljárással összhangban annak igazolása, hogy a természetes személy jogosult a minősített adathoz való hozzáférésre vagy a felhatalmazott szerv jogosult a minősített adat felhasználására;

c) „minősített adathoz való hozzáférés”: az a folyamat, amelynek során a Fél állama törvényeinek és egyéb jogszabályainak rendelkezéseivel összhangban erre felhatalmazott, megfelelő biztonsági tanúsítvánnyal rendelkező természetes személy a minősített adatot megismeri;

d) „szerződés”: a felhatalmazott szervek közötti megállapodás, amely abból a célból jött létre, hogy a köztük lévő együttműködés során a minősített adatok átadását és/vagy keletkezését szabályozza;

e) „a minősített adathordozó”: olyan tárgyi eszköz, beleértve a fizikai közegeket is, amely minősített adatot tartalmaz jelek, képek, jelzések, műszaki megoldások és folyamatok formájában;

f) „minősített adat”: valamennyi, a Felek állama törvényeinek és egyéb jogszabályainak rendelkezéseivel összhangban védett adat, amelyet valamelyik Fél és jelen Egyezmény által meghatározott eljárás szerint adtak át (vettek át), valamint amely a Felek közötti együttműködés során keletkezett, és amelynek jogosulatlan felhasználása valamely Fél állama biztonságának vagy érdekeinek sérelmével járhat;

g) „felhatalmazott szerv”: olyan állami szerv vagy szervezet (beleértve a gazdálkodó szervezeteket), amelyet valamelyik Fél a minősített adat átadására, átvételére, tárolására, védelmére és kezelésére hatalmazott fel.

2. Cikk

Hatáskörrel rendelkező hatóságok

(1) Jelen Egyezmény végrehajtásáért felelős, hatáskörrel rendelkező hatóságok (a továbbiakban: hatáskörrel rendelkező hatóságok) a következők:
- Magyarországon – a Nemzeti Biztonsági Felügyelet;
- az Oroszországi Föderációban – az Oroszországi Föderáció Szövetségi Biztonsági Szolgálata.

(2) A Felek haladéktalanul értesítik egymást diplomáciai úton a hatáskörrel rendelkező hatóságokkal kapcsolatos változásokról.

3. Cikk

A minősítési szintek megfeleltetése

(1) A Felek, államuk törvényeinek és egyéb jogszabályainak rendelkezései alapján megállapítják, hogy a minősítés szintjei és az azoknak megfelelő jelölések megfelelnek a következőknek:

Magyarországon:	Az Oroszországi Föderációban:
„Szigorúan titkos!”	Совершенно секретно
„Titkos!”	Секретно
„Bizalmas!”	Секретно
„Korlátozott terjesztésű!”	Секретно

(2) Az orosz Fél által átadott Секретно jelölésű minősített adathordozókat a magyar Fél „Titkos!” minősítési szintűként jelöli.

4. Cikk

A minősített adatok védelme

(1) A Felek, államuk törvényeinek és egyéb jogszabályainak rendelkezései alapján:
a) biztosítják a minősített adatok védelmét;
b) a minősített adat minősítési szintjét és a minősített adat hordozójának jelölését az átadó Fél felhatalmazott szervének írásbeli hozzájárulása nélkül nem változtatják meg;
c) a minősített adatok védelmére vonatkozóan ugyanolyan intézkedéseket kötelesek foganatosítani, mint amilyeneket saját minősített adataik vonatkozásában a 3. cikkben meghatározott megfeleltetés szerint az azonos minősítési szintre alkalmaznak;
d) a másik Fél felhatalmazott szervétől kapott minősített adatot kizárólag az átadás során meghatározott célra használják fel;
e) harmadik fél számára a minősített adathoz való hozzáférést csak az átadó Fél előzetes, írásbeli hozzájárulásával engedélyeznek.
(2) Minősített adathoz való hozzáférés csak azon személyek számára biztosítható, akiknek az adat megismerése az átadás során meghatározott célok eléréséhez előírt hivatali kötelességük teljesítéséhez szükséges, és akik megfelelő biztonsági tanúsítvánnyal rendelkeznek.

5. Cikk

A minősített adat átadása

(1) Ha az egyik Fél felhatalmazott szerve minősített adatot kíván átadni a másik Fél felhatalmazott szervének, a hatáskörrel rendelkező hatóságától a másik Fél felhatalmazott szerve biztonsági tanúsítványának meglétéről előzetes írásbeli igazolást kér.
Az átadó Fél hatáskörrel rendelkező hatósága az átvevő Fél hatáskörrel rendelkező hatóságától az átvevő Fél felhatalmazott szerve biztonsági tanúsítványának meglétéről szóló írásbeli igazolást kér.
Amennyiben az átvevő Fél felhatalmazott szervének biztonsági tanúsítványa visszavonásra kerül, az átvevő Fél hatáskörrel rendelkező hatósága értesíti az átadó Fél hatáskörrel rendelkező hatóságát.

(2) A minősített adat átadásáról az átadó Fél állama törvényeinek és egyéb jogszabályainak rendelkezéseivel összhangban kell dönteni.

(3) A minősített adathordozók átadása diplomáciai úton, futárral vagy a Felek által elfogadott egyéb felhatalmazott szolgáltató közreműködésével történhet. Az érintett felhatalmazott szerv megerősíti a minősített adat átvételét. A Felek a minősített adat átadásának egyéb, közösen megállapított módját is használhatják.

(4) Nagyszámú minősített adatot tartalmazó minősített adathordozó átadása esetén a felhatalmazott szervek államuk törvényeinek és egyéb jogszabályainak rendelkezéseivel összhangban megállapodnak a szállítás módjáról, az útitervről és a kíséret módjáról.

6. Cikk

A minősített adatok kezelése

(1) A minősített adat átvételéért felelős felhatalmazott szerv a 3. cikk szerinti minősítési szintet tünteti fel a minősített adathordozón.
A minősítési szint feltüntetésének kötelezettsége azon minősített adathordozók esetén is fennáll, amelyek a Felek közötti együttműködés során, valamint fordítás, másolás vagy sokszorosítás eredményeként keletkeztek.

Az átvett minősített adat alapján keletkezett minősített adathordozón feltüntetett minősítési szint nem lehet alacsonyabb, mint az átadott minősített adat minősítési szintje.

(2) A minősített adat kezelése, nyilvántartásba vétele és tárolása a Felek államában a minősített adatok vonatkozásában meghatározott követelményekkel összhangban történik.

(3) A minősített adathordozók megsemmisítése az átadó Fél felhatalmazott szervének írásbeli hozzájárulásával történik. A „Szigorúan titkos!”/ Совершенно секретно jelölésű minősített adathordozók nem semmisíthetők meg és az átadó Fél felhatalmazott szervéhez kell visszaküldeni őket, ha már nincs rájuk szükség.
A minősített adathordozók megsemmisítéséről dokumentáció készül és a megsemmisítés lefolytatása oly módon történik, hogy az adat újbóli létrehozása vagy visszaállítása ne legyen megvalósítható.
Az átadó Fél felhatalmazott szervét a minősített adathordozó megsemmisítéséről írásban értesíteni szükséges.

(4) Az átvett minősített adathordozó minősítési szintjét a felhatalmazott szerv kizárólag az átadó Fél felhatalmazott szervének előzetes írásbeli hozzájárulásával változtathatja meg vagy szüntetheti meg.
Az átadó Fél felhatalmazott szerve a másik Fél felhatalmazott szervét írásban értesíti az átadott minősített adat minősítési szintje megváltoztatásáról vagy megszüntetéséről.
A Felek együttműködése során keletkezett minősített adat minősítési szintje a felhatalmazott szervek kölcsönös egyetértésével állapítható meg, változtatható meg vagy szüntethető meg.

7. Cikk

Szerződések

A felhatalmazott szervek által kötött szerződések egy, a biztonságra vonatkozó külön mellékletet tartalmaznak, amely az alábbiakat foglalja magában:
a) a minősített adatok listáját és azok minősítési szintjét;
b) a minősített adathordozók védelmének, kezelésének, őrzésének és megsemmisítésének meghatározott követelményeit;
c) a vitás kérdések megoldásának rendjét és a minősített adat jogosulatlan terjesztéséből adódó esetleges károk megtérítésének kötelezettségét.

8. Cikk

A minősített adat védelmével kapcsolatos követelmények megsértése

(1) A Felek felhatalmazott szerve vagy hatáskörrel rendelkező hatósága haladéktalanul írásban értesíti a másik Fél érintett felhatalmazott szervét vagy hatáskörrel rendelkező hatóságát arról, ha a minősített adat védelmével kapcsolatos követelmények olyan megsértését azonosítja, amely az adat jogosulatlan terjesztéséhez vezet vagy vezethet.

(2) Az érintett felhatalmazott szerv vagy hatáskörrel rendelkező hatóság vizsgálatot folytat le és a vétkes személyeket az államuk törvényeinek és egyéb jogszabályainak rendelkezéseivel összhangban felelősségre vonja.

(3) A hatáskörrel rendelkező hatóságok írásban tájékoztatják egymást a vizsgálat eredményéről és a megvalósított intézkedésekről.

(4) A minősített adat jogosulatlan terjesztéséből származó esetleges károk enyhítésére szolgáló eljárásokat a Felek felhatalmazott szervei eseti jelleggel közösen határozzák meg.

9. Cikk

Látogatások

(1) Bármely Fél állama felhatalmazott szervei képviselőinek a másik Fél minősített adatához való hozzáférést igénylő látogatására csak a fogadó Fél állama törvényeinek és egyéb jogszabályainak rendelkezéseivel összhangban kerülhet sor.

(2) A látogatás lefolytatásának engedélyezésére irányuló kérelmet a küldő Fél felhatalmazott szerve küldi a fogadó Fél felhatalmazott szervének, főszabályként legalább 4 héttel a látogatás várható időpontját megelőzően. A látogatás lefolytatására irányuló engedély kiadásához a fogadó Fél hatáskörrel rendelkező hatóságának hozzájárulása szükséges. Sürgős esetben a Felek hatáskörrel rendelkező hatóságai a Felek állama törvényeinek és egyéb jogszabályainak rendelkezéseivel összhangban megtesznek minden lehetséges intézkedést a szükséges eljárások felgyorsítása érdekében.

(3) A tervezett látogatás lefolytatására irányuló kérelem az alábbi részleteket tartalmazza:
a) a küldő Fél felhatalmazott szerve képviselőjének vezeték- és keresztneve, születési ideje és helye, állampolgársága, útlevélszáma, munkahelye, beosztása és a biztonsági tanúsítványának szintje;
b) a meglátogatandó felhatalmazott szerv neve, címe és elérhetőségei;
c) a látogatás célja, alapja és a látogatással érintett legmagasabb minősítési szintű minősített adat minősítési szintje;
d) a látogatás időpontja és időtartama.

(4) A látogatás során az egyik Fél felhatalmazott szervének képviselője megismeri a másik Fél államának a minősített adatokkal kapcsolatos tevékenységére vonatkozó szabályait és megtartja azokat.

(5) A küldő Fél felhatalmazott szervének képviselője által, a látogatás során megismert minősített adatot úgy kell tekinteni, mint a jelen Egyezmény alapján átvett minősített adatot.

10. Cikk

A minősített adat védelmével kapcsolatos költségek

Jelen Egyezmény alapján a felhatalmazott szervek viselik a minősített adatok védelmével kapcsolatos intézkedések végrehajtásával kapcsolatos költségeket.

11. Cikk

Tájékoztatás nemzeti jogszabályokról és egyeztetések

(1) A hatáskörrel rendelkező hatóságok kellő időben kicserélik államuk minősített adatok védelmére vonatkozó törvényeit és egyéb jogszabályait, melyek ismerete jelen Egyezmény végrehajtásához szükséges.

(2) Jelen Egyezmény végrehajtása keretében, bármelyik Fél hatáskörrel rendelkező hatóságának kérelmére, az együttműködés biztosítása érdekében a hatáskörrel rendelkező hatóságok egyeztetéseket tartanak.

12. Cikk

Viták rendezése

(1) Jelen Egyezmény értelmezésével és alkalmazásával kapcsolatban felmerült viták a hatáskörrel rendelkező hatóságok közötti tárgyalások és egyeztetések útján rendezendőek.

(2) A viták rendezése idején a Felek továbbra is betartják jelen Egyezményből fakadó kötelezettségeiket.

13. Cikk

Módosítások

Jelen Egyezmény a Felek kölcsönös egyetértésével módosítható, erről szóló külön jegyzőkönyvek formájában, melyek hatálybalépése jelen Egyezmény hatálybalépésének megfelelő módon történik.

14. Cikk

Záró rendelkezések

(1) Jelen Egyezmény a Felek által az Egyezmény hatálybalépéséhez szükséges belső eljárások lefolytatásáról szóló, diplomáciai úton küldött utolsó írásbeli értesítés kézhezvételének napját követő második hónap első napján lép hatályba.

(2) Jelen Egyezmény határozatlan időre jött létre.

(3) Jelen Egyezményt bármelyik Fél jogosult felmondani az e döntésről szóló írásbeli értesítés másik Félhez, diplomáciai úton való megküldésével. Ebben az esetben jelen Egyezmény az értesítés kézhezvételének időpontját követő hatodik hónap elteltével hatályát veszti.
Jelen Egyezmény megszűnésekor a minősített adatok védelmére vonatkozóan a 4. és 6. cikkben meghatározott intézkedések alkalmazandók mindaddig, míg az adat minősítése a megfelelő eljárás szerint megszüntetésre kerül.

Készült Budapesten, 2016. szeptember 7-én, két példányban magyar, orosz és angol nyelven, valamennyi szöveg egyaránt hiteles. Bármilyen értelmezésbeli eltérés esetén az egyezmény angol nyelvű szövege alkalmazandó.

Magyarország Kormánya részéről

Az Oroszországi Föderáció Kormánya részéről

AGREEMENT BETWEEN THE GOVERNMENT OF HUNGARY AND THE GOVERNMENT OF THE RUSSIAN FEDERATION ON THE MUTUAL PROTECTION OF CLASSIFIED INFORMATION

The Government of Hungary and the Government of the Russian Federation, hereinafter referred to as the Parties,

Striving to ensure the protection of classified information exchanged in the course of political, military, military technical, economic or other cooperation, as well as of classified information generated in the process of such cooperation,

Taking into account mutual interests in ensuring the protection of classified information in accordance with the laws and other regulatory legal acts of the State of each Party,
Have agreed as follows:

Article 1
Use of Terms

The terms used in this Agreement shall have the following meaning:
a) “Classification marking” shall mean a mark indicated on the classified information carrier itself and/or on its accompanying documents, identifying the classification level of the information contained by the carrier;
b) “Security clearance” shall mean an individual’s right to have access to classified information or the right of an authorized body to use such information granted according to the procedure established by the laws and other regulatory legal acts of the State of each Party;
c) ”Access to classified information” shall mean the familiarization with classified information by an individual with an appropriate security clearance, authorized in accordance with the laws and other regulatory legal acts of the State of a Party;
d) “Contract” shall mean an agreement, concluded between the authorized bodies and providing for the transfer and/or generation of classified information in the course of cooperation.
e) ”Classified information carriers” shall mean material objects including physical fields, which contain classified information in the form of symbols, images, signals, engineering solutions and processes;
f) ”Classified information” shall mean any information protected in accordance with the laws and other regulatory legal acts of the State of each Party, transferred (received) according to the procedure established by each Party and this Agreement, as well as generated in the process of cooperation between the Parties, the unauthorized disclosure of which may damage the security or interests of the State of each Party;
g) “Authorized body” shall mean a public authority or an organization (including companies), authorized by a Party to transfer, receive, store, protect and use classified information.

Article 2
Competent Authorities

1. The competent authorities responsible for the implementation of this Agreement (hereinafter “the competent authorities”) shall be:

- in Hungary – National Security Authority;
- in the Russian Federation – Federal Security Service of the Russian Federation.

2. The Parties shall immediately notify each other through diplomatic channels of any change of their competent authorities.

Article 3
Comparability of Classification Levels

1. In accordance with the laws and other regulatory legal acts of their States, the Parties shall establish that classification levels and corresponding classification markings shall be comparable as follows:

in Hungary	in the Russian Federation
„Szigorúan titkos!”	Совершенно секретно
„Titkos!”	Секретно
„Bizalmas!”	Секретно
„Korlátozott terjesztésű!”	Секретно

2. The classified information carriers transferred by the Russian Party with the classification marking Секретно shall be marked by the Hungarian Party as „Titkos!”.

Article 4
Protection of Classified Information

1. In accordance with the laws and other regulatory legal acts of their States, the Parties shall:
a) ensure the protection of classified information;
b) not change the classification levels of classified information and a classification marking of classified information carriers without a written consent of the authorized body of the originating Party;
c) apply such protection measures to classified information as applicable to its own classified information with the same classification level, as comparable according to Article 3 hereof;
d) use classified information received from the authorized body of the other Party exclusively for the purposes envisaged in the course of its transfer;
e) not grant access to classified information to a third party without a prior written consent of the originating Party.

2. Access to classified information shall only be granted to the persons who need to know such information to perform their official duties for the purposes envisaged in the course of its transfer, and who have an appropriate security clearance.

Article 5
Transmission of Classified Information

1. If the authorized body of either Party intends to transfer classified information to the authorized body of the other Party, it shall ask the competent authority of its Party for a prior written confirmation of the security clearance of the other Party’s authorized body.
The competent authority of the originating Party shall request from the competent authority of the receiving Party a written confirmation of the security clearance of the receiving Party’s authorized body.
If the security clearance of the authorized body of the receiving Party is withdrawn, the competent authority of the receiving Party shall notify the competent authority of the originating Party.

2. The decision on transfer of classified information shall be taken in accordance with the laws and other regulatory legal acts of the State of the originating Party.
3. Classified information carriers shall be provided through diplomatic channels, courier or any authorized service in accordance with the arrangements made between the Parties. The respective authorized body shall confirm the receipt of classified information. The Parties may use other agreed methods of transfer of classified information.
4. For the transfer of classified information carriers of considerable volumes of classified information, the authorized bodies shall, in accordance with the laws and other regulatory legal acts of their States, agree on the modalities of their transportation, itinerary and escorting method.

Article 6
Handling of Classified Information

1. The authorized body responsible for receiving classified information shall additionally indicate the classification marking on the carrier in accordance with Article 3 hereof.
The requirement to indicate the classification marking shall apply to classified information carriers generated in the course of cooperation between the Parties, and as a result of translation, copying or reproduction.
The classification marking indicated on a classified information carrier generated on the basis of the classified information received, shall not be lower than that of the classified information transferred.
2. Classified information shall be handled, registered and stored by each Party in accordance with the requirements applicable to classified information of its State.
3. Classified information carriers shall be destroyed upon a written permission of the authorized body of the originating Party. Classified information carriers marked "Szigorúan titkos!"/ Совершенно секретно shall not be destroyed and shall be returned to the authorized body of the originating Party, when they are no longer deemed necessary.
Destruction of classified information carriers shall be documented and carried out in a way to exclude any reproduction or restoration of such information.
The authorized body of the originating Party shall be notified in writing of destruction of classified information carriers.
4. The authorized body may change or remove the classification marking of the received classified information carriers only upon a written permission of the authorized body of the originating Party.
The authorized body of the originating Party shall notify in writing the authorized body of the other Party concerning any change or removal of the classification marking of transferred classified information.
The classification level of the classified information generated in the course of cooperation between the Parties shall be determined, changed or annulled upon mutual consent of the authorized bodies.

Article 7
Contracts

The contracts concluded by the authorized bodies, shall include a separate section concerning security, which shall contain:
a) the list of classified information and its classification levels;
b) specific requirements regarding the protection, handling, storage and destruction of classified information carriers;
c) the procedure for dispute settlement and obligations to recover the possible damage from unauthorized dissemination of classified information.

Article 8

Violation of Requirements Regarding Protection of Classified Information

1. The authorized body or competent authority of a Party shall immediately inform in writing the respective authorized body or competent authority of the other Party of the identified violation of requirements regarding protection of classified information, which has led or may lead to its unauthorized dissemination.
2. The respective authorized body or competent authority shall carry out an investigation, and the person found guilty shall be held responsible in accordance with the laws and other regulatory legal acts of their State.
3. The competent authorities shall notify each other in writing of the results of the investigation and the measures taken.
4. The procedure for recovering possible damage from unauthorized dissemination of classified information shall be established on a case-by-case basis as agreed by the authorized bodies of the Parties.

Article 9
Visits

1. A visit of representatives of the authorized body of either Party involving their access to the classified information of the State of the other Party shall be made in accordance with the laws and other regulatory legal acts of the State of the receiving Party.
2. The request for permission to make the visit shall be filed by the authorized body of the sending Party to the authorized body of the receiving Party as a rule no later than 4 weeks before the expected date of visit. The permission to make the visit shall be agreed by the competent authority of the receiving Party. In urgent cases, the competent authorities of the Parties shall make all possible efforts to accelerate the necessary procedures in accordance with the laws and other regulatory legal acts of the State of each Party.
3. The request concerning the proposed visit shall contain the following details:
a) family and given names, date and place of birth, nationality, passport number, place of employment, position and level of security clearance of the representative of the authorized body of the sending Party;
b) name, address and contact details of authorized body to be visited;
c) purpose of visit, grounds for it and the highest security classification level of classified information involved;
d) date and duration of visit.
4. During the visit, the representative of the authorized body of a Party shall get familiarized with the rules of work with classified information of the State of the other Party and shall follow these rules.
5. Classified information acquired by the representative of the authorized body of the sending Party during the visit shall be considered as classified information received under this Agreement.

Article 10
Costs related to Protection of Classified Information

Authorized bodies shall bear the costs related to the implementation of measures for protection of classified information in accordance with this Agreement.

Article 11
Exchange of Regulatory Legal Acts and Consultations

1. The competent authority shall, in due course, exchange the appropriate laws and other regulatory legal acts of their States concerning the protection of classified information, which are necessary for implementation of this Agreement.
2. In order to ensure the cooperation, the competent authorities shall hold consultations within the framework of implementation of this Agreement at the request of either of them.

Article 12
Settlement of disputes

1. Disputes concerning the interpretation or application of this Agreement shall be settled through negotiations and consultations between the competent authorities.
2. The Parties shall continue to fulfil all their obligations hereunder in the course of dispute settlement.

Article 13
Amendments

Any amendments to this Agreement may be made by mutual agreement of the Parties, in the form of separate protocols, which shall come into force in the manner provided for entering into force of this Agreement.

Article 14
Final Provisions

1. This Agreement shall enter into force on the first day of the second month following the date of receipt of the last written notifications through diplomatic channels on completion of internal procedures by the Parties, necessary for this Agreement to enter into force.
2. This Agreement shall be concluded for an indefinite period of time.
3. Each Party may terminate this Agreement by sending a written notification of such decision to the other Party through diplomatic channels. In this case, this Agreement shall be terminated upon the expiry of six months from the date of receipt of such a notification.
In case of termination of this Agreement, the measures to protect classified information envisaged in Articles 4 and 6 hereof shall remain applicable until the information is declassified in due course.

Done at Budapest on 7th September 2016 in two copies, each in Hungarian, Russian and English languages, all texts being equally authentic. In case of any differences in interpretation of this Agreement the English text of the Agreement shall be used.

For the Government
of Hungary

For the Government
of the Russian Federation”

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 az Oroszországi Föderáció Kormánya között a minősített adatok kölcsönös védelméről szóló egyezmény kihirdetéséről szóló törvényjavaslathoz

Általános indokolás

Az Országgyűlés 2009. december 14-én fogadta el a minősített adat védelméről szóló 2009. évi CLV. törvényt (a továbbiakban: Mavtv.), amely az államtitokról és a szolgálati titokról szóló 1995. évi LXV. törvény, valamint a Nemzeti Biztonsági Felügyeletről szóló 1998. évi LXXXV. törvény helyébe lépett. A 2010. április 1-jétől hatályos új jogszabály alapjaiban kodifikálta újra a minősített adatok védelmének magyarországi struktúráját. Megteremtette a minősített adatok védelmének egységes jogszabály- és intézményrendszerét, s egyúttal eleget tett legfontosabb jogharmonizációs kötelezettségeinknek. A minősített adat védelméről szóló új törvény megalkotását indokolta az államtitokról és a szolgálati titokról szóló 1995. évi LXV. törvény átfogó felülvizsgálatának szükségessége: hiányoztak a külföldi (NATO, EU) és a nemzeti minősített adatok védelmére [elektronikus biztonságra (INFOSEC)] vonatkozó szabályok, az EU csatlakozásunk óta módosított EU normák átvételére, valamint az ehhez szükséges jogintézmények (a nemzeti személyi és telephely biztonsági tanúsítványok, nemzeti iparbiztonsági rendszer) bevezetésére nem került sor.

A minősített adatok cseréjére vonatkozó biztonsági együttműködés érdekében – a katonai megállapodások kivételével – hazánk jogszabályi felhatalmazás hiányában korábban csak két állammal kötött általános titokvédelmi egyezményt (*a Magyar Köztársaság Kormánya és az Olasz Köztársaság Kormánya között a minősített információk védelméről szóló, Budapesten, 2003. március 20-án aláírt Biztonsági Megállapodás kihirdetéséről szóló 2004. évi LXXXIX. törvény, valamint a Magyar Köztársaság Kormánya és Német Szövetségi Köztársaság Kormánya között a minősített információk kölcsönös védelme tárgyában Budapesten, 1995. október 25-én aláírt Egyezmény megerősítéséről és kihirdetéséről szóló 1996. évi XXXV. törvény),* amelyek alkalmazását a 2010. március 31-ig hatályos, az államtitokról és szolgálati titokról szóló 1995. évi LXV. törvény nem tette lehetővé.

A 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 kötött 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 Montenegróval.

2016. szeptember 7-én, Budapesten sor került *a Magyarország Kormánya és az Oroszországi Föderáció Kormánya között a minősített adatok cseréjéről és kölcsönös védelméről szóló egyezmény* (a továbbiakban: Egyezmény) aláírására, amelyre *a Magyarország Kormánya és az Oroszországi Föderáció Kormánya között a minősített adatok cseréjéről és kölcsönös védelméről szóló egyezmény szövegének végleges megállapítására adott felhatalmazásról szóló 1051/2016. (II. 15.) 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. Az Egyezmény 4. cikk (1) e) pontja szerint a Felek harmadik fél számára a minősített adathoz való hozzáférést csak az átadó Fél előzetes, írásbeli hozzájárulásával engedélyeznek. A Felek fogalma az Egyezmény preambulumából vezethető le, tehát megállapítható, hogy más titokvédelmi egyezményekhez hasonlóan harmadik fél bármely olyan állam, – beleértve a joghatósága alá tartozó jogi személyeket vagy természetes személyeket – vagy nemzetközi szervezet, amely nem részese jelen Egyezménynek.

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.