

MAGYARORSZÁG KORMÁNYA

**T/7756. számú
törvényjavaslat**

**a Cseh Köztársaság és Magyarország között a minősített adatok cseréjéről és kölcsönös
védelméről szóló egyezmény kihirdetéséről**

**Előadó: Dr. Navracsics Tibor
közigazgatási és igazságügyi
miniszter**

Budapest, 2012. június

2012. évi ... törvény

a Cseh Köztársaság és Magyarország között a minősített adatok cseréjéről és kölcsönös védelméről szóló egyezmény kihirdetéséről

1. §

Az Országgyűlés e törvénnyel felhatalmazást ad a Cseh Köztársaság és Magyarország között a minősített adatok cseréjéről és kölcsönös védelméről szóló egyezmény (továbbiakban: Egyezmény) kötelező hatályának elismerésére.

2. §

Az Országgyűlés az Egyezményt e törvénnyel kihirdeti.

3. §

Az Egyezmény hiteles angol és magyar nyelvű szövege a következő:

„AGREEMENT BETWEEN THE CZECH REPUBLIC AND HUNGARY ON THE EXCHANGE AND MUTUAL PROTECTION OF CLASSIFIED INFORMATION

The Czech Republic and Hungary (hereinafter referred to as the “Contracting Parties”)

Recognising the important role of the mutual cooperation between the Contracting Parties,

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

Recognising that they ensure equivalent protection for the Classified Information,

Wishing to ensure the protection of Classified Information exchanged between them or between legal entities or individuals under their jurisdiction,

Have, in mutual respect for national interests and security agreed upon the following:

ARTICLE 1 SCOPE OF THE AGREEMENT

1. The objective of this Agreement is to ensure the protection of Classified Information exchanged or generated in the course of co-operation between the Contracting Parties or between legal entities or individuals under their jurisdiction.
2. This Agreement shall not affect the obligations of the Contracting Parties under any other bilateral or multilateral treaty.
3. This Agreement shall not apply to the exchange of Classified Information between the intelligence services of the Contracting Parties.

ARTICLE 2 DEFINITIONS

For the purpose of this Agreement:

“Classified Information” means any information that, regardless of its form, under the national laws and regulations of either Contracting Party, requires protection against unauthorised disclosure, misappropriation or loss, and has been designated as such.

“Classified Contract” means a contract that contains or involves access to Classified Information.

“Originating Party” means the Contracting Party including legal entities or individuals under its jurisdiction, which releases Classified Information.

“Recipient Party” means the Contracting Party including legal entities or individuals under its jurisdiction, which receives Classified Information.

“Third Party” means any state including legal entities or individuals under its jurisdiction or international organisation not being a party to this Agreement.

ARTICLE 3 COMPETENT SECURITY AUTHORITIES

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

In the Czech Republic:

Národní bezpečnostní úřad

In Hungary:

Nemzeti Biztonsági Felügyelet

2. The Competent Security Authorities shall provide each other with official contact details and shall inform each other of any subsequent changes.

ARTICLE 4
SECURITY CLASSIFICATION LEVEL MARKINGS

The equivalence of national security classification level markings is as follows:

In the Czech Republic	In Hungary	Equivalent in the English language
PŘÍSNĚ TAJNÉ	SZIGORÚAN TITKOS	TOP SECRET
TAJNÉ	TITKOS	SECRET
DŮVĚRNÉ	BIZALMAS	CONFIDENTIAL
VYHRAZENÉ	KORLÁTOZOTT TERJESZTÉSŰ	RESTRICTED

ARTICLE 5
ACCESS TO CLASSIFIED INFORMATION

Access to Classified Information released under this Agreement shall be limited only to individuals duly authorized in accordance with the national laws and regulations of the respective Contracting 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 immediately of any subsequent changes in classification or declassification.

2. The Recipient Party shall:

- a) ensure that Classified Information is marked with equivalent security classification level marking in accordance with Article 4 of this Agreement;
- b) ensure the same level of protection to Classified Information as afforded to its national Classified Information of equivalent security classification level;
- c) ensure that Classified Information is not declassified nor its classification changed without the prior written consent of the Originating Party;
- d) ensure that Classified Information is not released to a Third Party without the prior written consent of the Originating Party;
- e) use Classified Information only for the purpose it has been released for and in accordance with handling requirements of the Originating Party.

ARTICLE 7 SECURITY CO-OPERATION

1. In order to maintain comparable standards of security, the Competent Security Authorities shall, on request, inform each other of their national laws and regulations concerning protection of Classified Information and the practices stemming from their implementation.
2. On request, the Competent Security Authorities shall, in accordance with their national laws and regulations, assist each other during the personnel security clearance procedures and facility security clearance procedures.
3. The Contracting Parties shall in accordance with national laws and regulations mutually recognise each other personnel security clearances and facility security clearances.
4. The Competent Security Authorities shall promptly notify each other about changes in recognised personnel security clearances and facility security clearances especially in cases of their revocation or termination.
5. In the course of the execution of this Agreement, Competent Security Authorities shall use the English language.

ARTICLE 8 CLASSIFIED CONTRACTS

1. Classified contracts shall be concluded and implemented in accordance with the national laws and regulations of respective Contracting Party. On request, the Competent Security Authorities shall confirm that proposed contractors as well as individuals participating in pre-contractual negotiations or in the implementation of Classified Contracts have appropriate personnel security clearance or facility security clearance.
2. The Competent Security Authorities may request that a security inspection is carried out at a facility located on the territory of the other Contracting Party to ensure continuing compliance with their national laws and regulations concerning protection of classified information.
3. Classified Contracts shall contain project security instruction on the security requirements and on the classification of each element of the Classified Contract. A copy of the project security instructions shall be forwarded to the Competent Security Authority of the Contracting Party under whose jurisdiction the Classified Contract is to be implemented.

ARTICLE 9 TRANSMISSION OF CLASSIFIED INFORMATION

1. Classified Information shall be transmitted in accordance with the national laws and regulations of the Originating Party through diplomatic channels or as otherwise agreed between the Competent Security Authorities.
2. The Contracting Parties may transmit Classified Information by electronic means in accordance with the security procedures approved by the Competent Security Authorities.

ARTICLE 10
REPRODUCTION, TRANSLATION AND DESTRUCTION OF CLASSIFIED
INFORMATION

1. Reproductions and translations of Classified Information released under this Agreement shall bear appropriate security classification markings and shall be protected as the original Classified Information. Number of reproductions shall be limited to the minimum needed.
2. Translations of Classified Information released under this Agreement shall bear a note in the language of translation indicating that they contain Classified Information of the Originating Party.
3. Classified Information released under this Agreement marked as PŘÍSNĚ TAJNÉ / SZIGORÚAN TITKOS / TOP SECRET shall be translated or reproduced only upon the prior written consent of the originator.
4. Classified Information released under this Agreement marked as PŘÍSNĚ TAJNÉ / SZIGORÚAN TITKOS / TOP SECRET shall not be destroyed and shall be returned to the Originating Party.

ARTICLE 11
VISITS

1. Visits requiring access to Classified Information shall be subject to the prior written consent of the respective Competent Security Authority, unless otherwise agreed between the Competent Security Authorities.
2. The visitor shall submit the request for visit at least twenty days in advance of the starting date of the visit to his national Competent Security Authority, which shall forward it to the Competent Security Authority of the other Contracting Party. In urgent cases, the request for visit may be submitted at a shorter notice, subject to prior co-ordination between the Competent Security Authorities.
3. Requests for visit shall include:
 - a) first and last name of the visitor, date and place of birth, nationality and passport/ID card number;
 - b) position of the visitor and specification of the facility, which the visitor represents;
 - c) visitor's personnel security clearance status and its validity;
 - d) date and duration of the visit, in case of recurring visit the total period of time covered by the visits shall be stated;
 - e) purpose of the visit including the highest level of Classified Information to be involved;
 - f) name, address, phone/fax number, e-mail address and point of contact of the facility to be visited;
 - g) date, signature and stamping of the official seal of the Competent Security Authority.
4. The Competent Security Authorities may agree on a list of visitors entitled to recurring visit. The Competent Security Authorities shall agree on the further details of the recurring visit.
5. Classified Information acquired by a visitor shall be considered as Classified Information released under this Agreement.

ARTICLE 12 BREACH OF SECURITY

1. The Competent Security Authorities shall immediately inform each other in writing of a breach of security resulting in unauthorised disclosure, misappropriation or loss of Classified Information or suspicion of such a breach.
2. The relevant security authorities of the Recipient Party shall investigate the incident without delay. The relevant security authorities of the Originating Party shall, if required, co-operate in the investigation.
3. In any case, the Recipient Party shall inform the Originating Party in writing about the circumstances of the breach of security, the extent of the damage, the measures adopted for its mitigation and the outcome of the investigation.

ARTICLE 13 EXPENSES

Each Contracting 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 Contracting Parties, through diplomatic channels, stating that the internal legal procedures for this Agreement to enter into force have been fulfilled.
2. This Agreement may be amended on the basis of the mutual consent of the Contracting Parties. Such amendments shall enter into force in accordance with paragraph 1 of this Article.
3. Each Contracting Party is entitled to terminate this Agreement in writing at any time. In such a case, the validity of the Agreement shall expire after six months following the day on which the other Contracting Party receives the written notice of the termination.
4. Regardless of the termination of this Agreement, all Classified Information released 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.
5. Any dispute regarding the interpretation or implementation of this Agreement shall be resolved by consultations and negotiations between the Contracting 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 13 June 2012 in two originals, in the Czech, Hungarian and English languages, each text being equally authentic. In case of different interpretation the English text shall prevail.

For the Czech Republic

For Hungary

EGYEZMÉNY A CSEH KÖZTÁRSASÁG ÉS MAGYARORSZÁG KÖZÖTT A MINŐSÍTETT ADATOK CSERÉJÉRŐL ÉS KÖLCSÖNÖS VÉDELMEÉRŐL

A Cseh Köztársaság és Magyarország (a továbbiakban együtt: Szerződő Felek)

Elismerve a Szerződő Felek közötti kölcsönös együttműködés fontos szerepét,

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

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

Kíváncsún tartva, hogy a közöttük, illetve a joghatóságuk alá tartozó jogi személyek és természetes személyek között kicserélt minősített adatok megfelelő védelemben részesüljenek,

Kölcsönösen tiszteletben tartva egymás nemzeti érdekeit és biztonságát, az alábbiakban állapodtak meg:

1. Cikk

Az Egyezmény tárgya

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

2. Az Egyezmény nem érinti a Szerződő Felek egyéb két-, vagy többoldalú szerződés alapján fennálló kötelezettségeit.

3. Jelen Egyezmény rendelkezéseit nem kell alkalmazni a Szerződő Felek hírszerző szolgálatainak között kicserélt minősített adatok vonatkozásában.

2. Cikk

Fogalom meghatározások

Jelen Egyezmény alkalmazásában:

A „**Minősített Adat**” megjelenési formájától függetlenül, minden olyan adat, amelyet bármelyik Szerződő Fél nemzeti jogszabályai szerint védelemben kell részesíteni a jogosulatlan hozzáféréssel, jogosulatlan felhasználással, illetve elvesztésével szemben, s amelyet ennek megfelelően minősítettek.

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

Az „**Átadó Fél**” azt a Szerződő Felet, illetve a joghatósága alá tartozó jogi személyeket vagy természetes személyeket jelenti, amelyek a minősített adatot átadja.

Az „**Átvevő Fél**” azt a Szerződő Felet, illetve a joghatósága alá tartozó jogi személyeket vagy természetes személyeket jelenti, amelyek a minősített adatot átveszi.

A „**Harmadik Fél**” bármely olyan államot, illetve a joghatósága alá tartozó jogi személyeket vagy természetes személyeket, továbbá nemzetközi szervezetet jelent, amely nem részese jelen Egyezménynek.

3. Cikk

A hatáskörrel rendelkező biztonsági hatóságok

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

A Cseh Köztársaságban:

Národní Bezpečnostní Úřad

Magyarországon:

Nemzeti Biztonsági Felügyelet

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

4. Cikk

Minősítési szintek megfeleltetése

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

A Cseh Köztársaságban	Magyarországon	Angol nyelvű megfelelőjük
PŘÍSNĚ TAJNÉ	SZIGORÚAN TITKOS	TOP SECRET
TAJNÉ	TITKOS	SECRET
DŮVĚRNÉ	BIZALMAS	CONFIDENTIAL
VYHRAZENÉ	KORLÁTOZOTT TERJESZTÉSŰ	RESTRICTED

5. Cikk

Minősített adathoz való hozzáférés

A jelen Egyezmény alapján átadott minősített adathoz kizárólag olyan személyek jogosultak hozzáférni, akik az adott Szerződő Fél nemzeti jogszabályaival összhangban erre megfelelő felhatalmazást kaptak.

6. Cikk

Biztonsági alapelvek

1. Az Átadó Fél:

- a) köteles biztosítani, hogy a minősített adaton a nemzeti jogszabályai szerinti megfelelő minősítési szint feltüntetésre kerüljön;
- b) köteles tájékoztatni az Átvevő Felet a minősített adat felhasználásának esetleges feltételhez kötöttségéről;
- c) haladéktalanul köteles tájékoztatni az Átvevő Felet az adat minősítésében bekövetkezett változásokról, illetve a minősítés megszüntetéséről.

2. Az Átvevő Fél:

- a) köteles biztosítani, hogy a minősített adaton feltüntetésre kerüljön a jelen Egyezmény 4. Cikke alapján meghatározott egyenértékű minősítési szint;
- b) ugyanolyan szintű védelemben köteles részesíteni a minősített adatot, mint amelyet a saját, azonos minősítési szintű nemzeti minősített adata számára biztosít;
- c) a köteles biztosítani, hogy az Átadó Fél előzetes írásbeli hozzájárulása nélkül az átvett minősített adat minősítését nem szüntetik meg, illetve minősítési szintjét nem változtatják meg;
- d) köteles biztosítani, hogy az Átadó Fél előzetes írásbeli hozzájárulása nélkül az átvett minősített adathoz Harmadik Fél nem fér hozzá;
- e) a minősített adatot kizárólag az átadás során megjelölt célra használhatja fel, betartva az Átadó Fél által meghatározott kezelési előírásokat.

7. Cikk

Biztonsági együttműködés

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

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

3. A Szerződő Felek nemzeti jogszabályaik rendelkezéseivel összhangban kölcsönösen elismerik egymás személyi biztonsági tanúsítványait és telephely biztonsági tanúsítványait.

4. A hatáskörrel rendelkező biztonsági hatóságok haladéktalanul értesítik egymást az elismert személyi biztonsági tanúsítványokkal és a telephely biztonsági tanúsítvánnyal kapcsolatos változásokról, különösen azok visszavonásáról, valamint érvényességi idejük lejártáról.

5. A jelen Egyezmény végrehajtása során a hatáskörrel rendelkező biztonsági hatóságok az angol nyelvet használják.

8. Cikk

Minősített szerződések

1. A minősített szerződéseket a Szerződő Felek saját nemzeti jogszabályai alapján kell megkötni és teljesíteni. A hatáskörrel rendelkező biztonsági hatóságok megkeresésre kötelesek megerősíteni, hogy az ajánlattevő és az előzetes szerződési tárgyalásokban vagy a minősített szerződések teljesítésében részt vevő természetes személyek rendelkeznek-e megfelelő személyi biztonsági tanúsítvánnyal vagy telephely biztonsági tanúsítvánnyal.
2. A hatáskörrel rendelkező biztonsági hatóságok kérhetik, hogy a másik Szerződő Fél biztonsági ellenőrzést folytasson le a területén működő létesítményben a minősített adat védelmére vonatkozó jogszabályoknak való folyamatos megfelelés ellenőrzése céljából.
3. A minősített szerződések részét képezi a projekt biztonsági utasítás, amely a biztonsági követelményeket és a szerződés egyes elemeinek minősítésével kapcsolatos rendelkezéseket határozza meg. A projekt biztonsági utasítás másolatát azon hatáskörrel rendelkező biztonsági hatóság részére kell továbbítani, amelynek joghatósága alatt a minősített szerződés végrehajtása történik.

9. Cikk

A minősített adat továbbítása

1. A minősített adat továbbítása az Átadó Fél nemzeti jogszabályaiban meghatározott szabályok szerint, diplomáciai úton, vagy a hatáskörrel rendelkező biztonsági hatóságok által közösen meghatározott egyéb módon történik.
2. A Szerződő Felek a hatáskörrel rendelkező biztonsági hatóságok által jóváhagyott eljárási rend szerint, elektronikus úton is továbbíthatnak minősített adatot.

10. Cikk

A minősített adat sokszorosítása, fordítása és megsemmisítése

1. Jelen Egyezmény alapján átadott minősített adatról készült másolatokon és fordításokon fel kell tüntetni a megfelelő minősítési jelölést és az így készült adatot ugyanolyan védelemben kell részesíteni, mint az eredeti minősített adatot. A sokszorosított példányok számát a szükséges minimumra kell korlátozni.
2. Jelen Egyezmény alapján átadott minősített adat fordítása során keletkező példányokon a fordítás nyelvén fel kell tüntetni, hogy az az Átadó Fél minősített adatát tartalmazza.
3. Jelen Egyezmény alapján átadott PŘÍSNĚ TAJNĚ/SZIGORÚAN TITKOS/TOP SECRET minősítésű adat fordítása vagy sokszorosítása kizárólag a minősítő előzetes írásbeli engedélyével lehetséges.
4. Jelen Egyezmény alapján átadott PŘÍSNĚ TAJNĚ/SZIGORÚAN TITKOS/TOP SECRET minősítésű adat nem semmisíthető meg, az ezen minősítési szintű adatokat az Átadó Félnek kell visszaszolgáltatni.

11. Cikk

Látogatások

1. Minősített adathoz való hozzáférést igénylő látogatásra az érintett hatáskörrel rendelkező biztonsági hatóság előzetes írásbeli jóváhagyása alapján kerül sor, amennyiben a hatáskörrel rendelkező biztonsági hatóságok másképp nem állapodtak meg.

2. A látogató a látogatásra vonatkozó megkeresést legalább 20 nappal a látogatás megkezdésének tervezett időpontja előtt a hatáskörrel rendelkező biztonsági hatóságához nyújtja be, amely azt továbbítja a másik Szerződő Fél hatáskörrel rendelkező biztonsági hatóságához. Sürgős esetben, a hatáskörrel rendelkező biztonsági hatóságok előzetes egyeztetését követően a látogatásra vonatkozó megkeresés a látogatás kezdetéhez közelebbi időpontban is benyújtható.

3. A látogatásra vonatkozó megkeresésnek az alábbiakat kell tartalmaznia:

- a) a látogató családi és utóneve, születési helye és ideje, állampolgársága, útlevelének vagy más személyazonosító igazolványának száma;
- b) a látogató beosztásának és a látogató által képviselt létesítmény megjelölése;
- c) a látogató személyi biztonsági tanúsítványának szintje és érvényességi ideje;
- d) a látogatás időpontja és időtartama, visszatérő látogatások esetén az egyes látogatások összesített időtartama;
- e) a látogatás célja, valamint a megismerendő legmagasabb minősítési szintű minősített adat minősítési szintjének megjelölése;
- f) a meglátogatandó létesítmény neve, címe, telefonszáma, fax száma, e-mail címe, valamint kapcsolattartójának neve;
- g) dátum, aláírás és a hatáskörrel rendelkező biztonsági hatóság hivatalos pecsétjének lenyomata.

4. A hatáskörrel rendelkező biztonsági hatóságok közösen meghatározhatják a visszatérő látogatásra jogosult személyek listáját. A visszatérő látogatások további részleteit a hatáskörrel rendelkező biztonsági hatóságok közösen állapítják meg.

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

12. Cikk

Eljárás a minősített adat biztonságának megsértése esetén

1. A hatáskörrel rendelkező biztonsági hatóságok haladéktalanul írásban tájékoztatják egymást azon minősített adat biztonságának megsértéséről, amely esetében a minősített adathoz való jogosulatlan hozzáférésre, a minősített adat jogosulatlan felhasználására vagy elvesztésére kerül sor, vagy mindezek alapos gyanúja merül fel.

2. Az Átvevő Fél feladat- és hatáskörrel rendelkező biztonsági hatóságai késedelem nélkül intézkednek a minősített adat biztonsága megsértésének kivizsgálása érdekében. Az Átadó Fél feladat- és hatáskörrel rendelkező biztonsági hatóságai szükség esetén részt vesznek a vizsgálatban.

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

13. Cikk

Költségek viselése

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

14. Cikk

Záró rendelkezések

1. Jelen Egyezmény határozatlan időre jön létre. Jelen Egyezmény a Szerződő Felek az Egyezmény hatálybalépéséhez szükséges belső feltételek teljesítésére vonatkozó, diplomáciai úton küldött utolsó értesítése kézhezvételének napját követő második hónap első napján lép hatályba.

2. Jelen Egyezmény a Szerződő Felek kölcsönös egyetértésével módosítható. A módosítások hatálybalépésével kapcsolatban a jelen cikk 1. pontjában foglaltak az irányadók.

3. Bármelyik Szerződő Fél jogosult jelen Egyezményt bármikor írásban felmondani. Felmondás esetén az Egyezmény a felmondásról szóló írásbeli értesítés másik Szerződő Fél általi kézhezvételétől számított 6 hónap elteltével hatályát veszti.

4. Az Egyezmény megszűnésétől függetlenül az annak alapján átadott vagy keletkeztetett minősített adatokat az Egyezményben meghatározott rendelkezések szerint kell védelemben részesíteni, mindaddig, amíg az Átadó Fél felmentést nem ad az Átvevő Fél részére ezen kötelezettség alól.

5. Szerződő Felek a jelen Egyezmény értelmezéséből vagy végrehajtásából fakadó vitákat tárgyalás és egyeztetés útján, külső jogszolgáltatási fórum igénybe vétele nélkül rendezik.

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

Készült Budapesten, 2012. június 13-án, két eredeti példányban, cseh, magyar és angol nyelven, mindhárom szöveg egyaránt hiteles. Eltérés esetén az angol nyelvű szöveg az irányadó.

.....
a Cseh Köztársaság részéről

.....
Magyarország részéről”

4. §

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

(2) A 2. és 3. § az Egyezmény 14. Cikk 1. pontjában meghatározott időpontban lép hatályba.

- (3) Az Egyezmény, illetve e törvény 2. és 3. §-a hatálybalépésének naptári napját a külpolitikáért felelős miniszter annak ismertté válását követően a Magyar Közlönyben haladéktalanul közzétett közleményével állapítja meg.
- (4) E törvény végrehajtásához szükséges intézkedésekről a minősített adatok védelmének szakmai felügyeletéért felelős miniszter gondoskodik.

**INDOKOLÁS A CSEH KÖZTÁRSASÁG ÉS MAGYARORSZÁG KÖZÖTT A MINŐSÍTETT
ADATOK CSERÉJÉRŐL ÉS KÖLCSÖNÖS VÉDELMEÉRŐL SZÓLÓ EGYEZMÉNY
KIHIRDETÉSÉRŐL SZÓLÓ TÖRVÉNYJAVASLATHOZ**

ÁLTALÁNOS INDOKOLÁS

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

Jogszabályi felhatalmazás hiányában a minősített adatok cseréjére vonatkozó biztonsági együttműködés érdekében hazánk a mai napig két állammal kötött általános titokvédelmi megállapodást (*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. októberben 25-én aláírt Egyezmény megerősítéséről és kihirdetéséről szóló 1996. évi XXXV. törvény*), amelyek alkalmazását azonban az államtitokról és szolgálati titokról szóló 1995. évi LXV. törvény nem tette lehetővé a hiányzó jogintézmények – nemzeti személyi biztonsági tanúsítvány, nemzeti telephely biztonsági tanúsítvány – okán.

A Mavtv. hatálybalépésével azonban megteremtette a kétoldalú titokvédelmi megállapodások megkötéséhez és alkalmazásához szükséges jogi alapokat. Az Egyezmény megkötése a Mavtv.-ben foglaltak végrehajtása, Magyarország nemzetközi kötelezettségvállalásainak teljesítése, továbbá a

minősített adatok cseréjével járó nemzetközi biztonsági együttműködésekben történő részvétel szükségessége miatt is indokolt.

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. 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 az angol és magyar nyelvű hiteles szövegét.

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

A 4. §-hoz

A Javaslat a kihirdetését követő napon lép hatályba. A (2) bekezdésben foglalt kivétel indoka, az Egyezmény kötelező hatályának elismerésére a Felek által alkalmazandó alkotmányos vagy belső jogi szabályokkal és eljárásokkal összhangban kerüljön sor. Az Egyezmény 14. cikk (1) bekezdése szerint a *„Jelen Egyezmény a Szerződő Felek az Egyezmény hatálybalépéshez szükséges belső feltételek teljesítésére vonatkozó, diplomáciai úton küldött utolsó értesítése kézhezvételének napját követő második hónap első napján lép hatályba.”*

Az Egyezmény hatálybalépésének naptári napját a külpolitikáért felelős miniszter annak ismertté válását követően a Magyar Közlönyben közzétett közleményével állapítja meg.