MAGYARORSZÁG KORMÁNYA

T/8569. számú

törvényjavaslat

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

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

Budapest, 2012. szeptember

2012. évi ... törvény

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

1. §

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

2. §

Az Országgyűlés az Egyezményt e törvénnyel kihirdeti.

3. §

Az Egyezmény hiteles angol és magyar nyelvű szövege a következő:

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

The Government of Hungary and the Government of the Republic of Latvia (hereinafter referred to as the "Contracting Parties"),

Recognising the important role of the mutual cooperation,

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 obligation of the Contracting Parties under any other bilateral or multilateral treaty, including any agreements governing exchange and mutual protection of Classified Information.

ARTICLE 2
DEFINITIONS

For the purpose of this Agreement:

a) **"Classified Information"** means any information that, regardless of its form or nature, under the national laws and regulations of either Contracting Party, requires protection against unauthorised disclosure or any other unauthorized manipulation and has been duly designated.

b) **"Classified Contract"** means a contract that involves or requires access to Classified Information.

c) **"Originating Party"** means the Contracting Party including legal entities or individuals under its jurisdiction, which releases Classified Information.

d) **"Recipient Party"** means the Contracting Party including legal entities or individuals under its jurisdiction, which receives Classified Information.

e) **"Third Party"** means any state including legal entities or individuals under its jurisdiction or international organisation not being a party to this Agreement.

f) **"Facility Security Clearance"** means a determination by a Competent Security Authority of a Contracting Party that a Contractor located in its country is security cleared and has in place appropriate security measures within a specific facility to access and protect Classified Information in accordance with its national laws and regulations.

g) **"Personnel Security Clearance"** means a determination by a Competent Security Authority of a Contracting Party that an individual has been security cleared to access and handle Classified Information in accordance with its national laws and regulations.

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 Hungary:

National Security Authority

In the Republic of Latvia:

Constitution Protection Bureau

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

ARTICLE 4
SECURITY CLASSIFICATION LEVELS AND MARKINGS

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

In Hungary	**In the Republic of Latvia**	**Equivalent in the English language**
SZIGORÚAN TITKOS	SEVIŠĶI SLEPENI	TOP SECRET
TITKOS	SLEPENI	SECRET
BIZALMAS	KONFIDENCIĀLI	CONFIDENTIAL
KORLÁTOZOTT TERJESZTÉSŰ	DIENESTA VAJADZĪBĀM	RESTRICTED

ARTICLE 5
ACCESS TO CLASSIFIED INFORMATION

Access to Classified Information under this Agreement shall be limited only to individuals duly authorised in accordance with the national laws and regulations of the respective 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 without undue delay of any subsequent changes in the security classification level.

2. The Recipient Party shall:
a) ensure that Classified Information is marked with an equivalent security classification marking in accordance with Article 4;
b) afford the same degree of protection to Classified Information as afforded to its own Classified Information of an equivalent security classification level;
c) ensure that Classified Information is not declassified nor its security classification level changed without the prior written consent of the Originating Party;
d) ensure that Classified Information is not released to a Third Party without the prior written consent of the Originating Party;
e) use Classified Information only for the purpose it has been released for and in accordance with release conditions of the Originating Party.

ARTICLE 7
SECURITY CO-OPERATION

1. In order to maintain comparable standards of security, the Competent Security Authorities shall, on request, inform each other of their national laws and regulations concerning protection of Classified Information and the practices stemming from their implementation. The Competent Security Authorities shall inform each other of any substantive changes of their national laws and regulations concerning this Agreement.

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 on request and in accordance with their national laws and regulations, recognise the Personnel Security Clearance certificates and Facility Security Clearance certificates issued by the other Contracting Party. Article 4 of this Agreement shall apply accordingly.

4. The Competent Security Authorities shall promptly notify each other about changes in the recognised Personnel Security Clearance certificates and Facility Security Clearance certificates, especially in case of their withdrawal.

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

ARTICLE 8
CLASSIFIED CONTRACTS

1. Classified contracts shall be concluded and implemented in accordance with the national laws and regulations of each Contracting Party. On request, the Competent Security Authorities shall confirm if the proposed contractors as well as individuals participating in pre-contractual negotiations or in the implementation of Classified Contracts have an appropriate Personnel Security Clearance certificate or Facility Security Clearance certificate.

2. The Competent Security Authority may request its counterpart that a security inspection is carried out at a facility located in the territory of the other Contracting Party to ensure continuing protection of Classified Information.

3. Classified Contracts shall contain project security instructions on the security requirements and on the security classification level of each element of the Classified Contract. A copy of the project security instructions shall be forwarded to the Competent Security Authority of the 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 in executive protocols.

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 originals. Number of reproductions shall be limited to that required for official purposes.

2. Translations of Classified Information released under this Agreement shall bear a note in the language of translation indicating that they contain Classified Information of the Originating Party.

3. Classified Information released under this Agreement marked SZIGORÚAN TITKOS/ SEVIŠĶI SLEPENI/ TOP SECRET shall be translated or reproduced only upon the prior written consent of the Originating Party.

4. Classified Information released under this Agreement marked SZIGORÚAN TITKOS/ SEVIŠĶI SLEPENI/ 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 Competent Security Authority of the Recipient Party.

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

3. Requests for visit shall contain:
a) visitor's name, date and place of birth, nationality and passport/ID card number;
b) position of the visitor and specification of the legal entity represented;
c) visitor's Personnel Security Clearance certificate status and its validity;
d) date and duration of the visit; in case of recurring visits the total period of time covered by the visits;
e) purpose of the visit including the highest security classification level of Classified Information involved;
f) name and address of the facility to be visited, as well as the name, phone/fax number, e-mail address of its point of contact;
g) date, signature and stamping of the official seal of the Competent Security Authority.

4. The Competent Security Authorities may agree on a list of visitors entitled to recurring visits. The Competent Security Authorities shall agree on the further details of the recurring visits.

5. Classified Information acquired by a visitor shall be considered as Classified Information received under this Agreement.

ARTICLE 12
BREACH OF SECURITY

1. The Competent Security Authorities shall without undue delay inform each other in writing of a breach of security resulting in unauthorised disclosure or any other unauthorised manipulation of Classified Information under this Agreement or suspicion thereof.

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

3. In any case, the Competent Security Authority of the Recipient Party shall inform the Competent 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 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 national legal requirements for this Agreement to enter into force have been fulfilled.

2. This Agreement may be amended on the basis of the mutual agreement of the Contracting Parties in writing. 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 this 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 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 Contracting Parties, without recourse to outside jurisdiction.

Done in Budapest on 29 August 2012 in two originals, in Hungarian, Latvian and English languages, each text being equally authentic. In case of different interpretation the English text shall prevail.

For the Government of Hungary	**For the Government of the Republic of Latvia**

EGYEZMÉNY MAGYARORSZÁG KORMÁNYA ÉS A LETT KÖZTÁRSASÁG KORMÁNYA KÖZÖTT A MINŐSÍTETT ADATOK CSERÉJÉRŐL ÉS KÖLCSÖNÖS VÉDELMÉRŐL

Magyarország Kormánya és a Lett Köztársaság Kormánya (a továbbiakban együtt: Szerződő Felek)

Elismerve a 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,

Kívánatosnak 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, beleértve ebbe mindazon megállapodásokat, amelyek minősített adatok cseréjét és kölcsönös védelmét szabályozzák.

2. Cikk
Fogalommeghatározások

Jelen Egyezmény alkalmazásában:

a) A **„Minősített Adat"** megjelenési formájától vagy természetétől függetlenül minden olyan adat, amelyet bármelyik Szerződő Fél nemzeti jogszabályai szerint védelemben kell részesíteni a jogosulatlan hozzáféréssel vagy jogosulatlan megváltoztatással szemben, és amelyet ennek megfelelően minősítettek.

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

c) Az **„Átadó Fél"** azt a Szerződő Felet, valamint a joghatósága alá tartozó jogi személyeket vagy természetes személyeket jelenti, amely a minősített adatot átadja.

d) Az **„Átvevő Fél"** azt a Szerződő Felet, valamint a joghatósága alá tartozó jogi személyeket vagy természetes személyeket jelenti, amely a minősített adatot átveszi.

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

f) A **„Telephely Biztonsági Tanúsítvány"** valamely Szerződő Fél hatáskörrel rendelkező biztonsági hatóságának azon döntése, amellyel megállapítja, hogy a területén tevékenykedő szerződő biztonsági szempontú átvilágítása megtörtént, a minősített adat kezelése biztonsági kockázattal nem jár, telephelyén a minősített adathoz történő hozzáférés és a minősített adat védelme érdekében a szükséges biztonsági intézkedéseket a nemzeti jogszabályokkal összhangban megtette.

g) A **„Személyi Biztonsági Tanúsítvány"** valamely Szerződő Fél hatáskörrel rendelkező biztonsági hatóságának azon döntése, amellyel megállapítja, hogy egy személy biztonsági szempontú átvilágítása megtörtént és a minősített adathoz történő hozzáférése, vagy a minősített adat általa történő kezelése a nemzeti jogszabályokkal összhangban biztonsági kockázattal nem jár.

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:

Magyarországon:

Nemzeti Biztonsági Felügyelet

A Lett Köztársaságban:

Constitution Protection Bureau

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:

Magyarországon	**A Lett Köztársaságban**	**Angol nyelvű megfelelőjük**
SZIGORÚAN TITKOS	SEVIŠĶI SLEPENI	TOP SECRET
TITKOS	SLEPENI	SECRET
BIZALMAS	KONFIDENCIĀLI	CONFIDENTIAL
KORLÁTOZOTT TERJESZTÉSŰ	DIENESTA VAJADZĪBĀM	RESTRICTED

5. Cikk
Minősített adathoz való hozzáférés

Minősített adathoz jelen Egyezmény alapján 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 kötéséről;
c) haladéktalanul köteles tájékoztatni az Átvevő Felet az adat minősítésében bekövetkezett változásokról.

2. Az Átvevő Fél:
a) köteles biztosítani, hogy a minősített adaton feltüntetésre kerüljön a 4. Cikk alapján meghatározott egyenértékű minősítési szint;
b) ugyanolyan szintű védelemben köteles részesíteni a minősített adatot, mint amelyet a saját, azonos minősítési szintű minősített adata számára biztosít;
c) köteles biztosítani, hogy az Átadó Fél előzetes írásbeli hozzájárulása nélkül az átvett minősített adat minősítését nem szüntetik meg, illetve minősítési szintjét nem változtatják meg;
d) köteles biztosítani, hogy az Átadó Fél előzetes írásbeli hozzájárulása nélkül az átvett minősített adatot Harmadik Fél részére nem adja át;
e) a minősített adatot kizárólag az átadás során megjelölt célra használhatja fel, betartva az Átadó Fél által meghatározott kezelési előírásokat.

7. Cikk
Biztonsági együttműködés

1. A hasonló szintű biztonsági követelmények fenntartása érdekében a hatáskörrel rendelkező biztonsági hatóságok a másik fél megkeresésére kötelesek egymást tájékoztatni a minősített adat védelmével kapcsolatos nemzeti jogszabályokról, valamint mindezek gyakorlati alkalmazásáról. A hatáskörrel rendelkező biztonsági hatóságok tájékoztatják továbbá egymást minden, a nemzeti jogszabályaikat érintő, jelen Egyezménnyel kapcsolatos lényeges változásról.

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 megkeresés esetén nemzeti jogszabályaik rendelkezéseivel összhangban elismerik a másik Szerződő Fél által kibocsátott személyi biztonsági tanúsítványokat és telephely biztonsági tanúsítványokat. Mindezek során a jelen Egyezmény 4. Cikkében foglaltakat megfelelően kell alkalmazni.

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

5. 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 kérelmezhetik, hogy a másik Szerződő Fél biztonsági ellenőrzést folytasson le a területén működő létesítményben a minősített adat folyamatos védelmének biztosítása céljából.

3. A minősített szerződések részét képezi a projekt biztonsági utasítás, amely a biztonsági követelményeket és a szerződés egyes elemeinek minősítésével kapcsolatos rendelkezéseket határozza meg. A projekt biztonsági utasítás másolatát azon Szerződő Fél hatáskörrel rendelkező biztonsági hatósága részére kell továbbítani, amelynek joghatósága alatt a minősített szerződés végrehajtása történik.

9. Cikk
A minősített adat továbbítása

1. A minősített adat továbbítása az Átadó Fél nemzeti jogszabályaiban meghatározott szabályok szerint, diplomáciai úton, vagy a hatáskörrel rendelkező biztonsági hatóságok által végrehajtási utasításokban közösen meghatározott egyéb módon történik.

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 hivatalos célból szükséges mértékre kell korlátozni.

2. Jelen Egyezmény alapján átadott minősített adat fordítása során keletkező példányokon a fordítás nyelvén fel kell tüntetni, hogy az Átadó Fél minősített adatát tartalmazza.

3. Jelen Egyezmény alapján átadott, SZIGORÚAN TITKOS/ SEVIŠKI SLEPENI /TOP SECRET minősítésű adat fordítása vagy sokszorosítása kizárólag az Átadó Fél előzetes írásbeli engedélyével lehetséges.

4. Jelen Egyezmény alapján átadott, SZIGORÚAN TITKOS/ SEVIŠKI SLEPENI /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 a fogadó Szerződő Fél hatáskörrel rendelkező biztonsági hatóságának előzetes írásbeli jóváhagyása alapján kerülhet sor.

2. A látogatásra vonatkozó megkeresést legalább 20 nappal a látogatás időpontja előtt a hatáskörrel rendelkező biztonsági hatósághoz kell benyújtani, amely azt továbbítja a fogadó 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 neve, 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 és címe, valamint a kapcsolattartójának neve, telefonszáma, fax száma, e-mail címe;
g) dátum, aláírás és a hatáskörrel rendelkező biztonsági hatóság hivatalos pecsétjének lenyomata.

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

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

12. Cikk
Eljárás a minősített adat biztonságának megsértése esetén

1. A hatáskörrel rendelkező biztonsági hatóságok késedelem nélkül írásban tájékoztatják egymást azon minősített adat biztonságának megsértéséről, amely esetben a jelen Egyezmény hatálya alá tartozó minősített adathoz való jogosulatlan hozzáférésre, a minősített adat jogosulatlan megváltoztatására kerül sor, vagy mindezek alapos gyanúja merül fel.

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

3. Az Átvevő Fél hatáskörrel rendelkező biztonsági hatósága minden esetben írásban tájékoztatja az Átadó Fél hatáskörrel rendelkező biztonsági hatóságát 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 írásban 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 írásban felmentést nem ad az Átvevő Fél részére ezen kötelezettség alól.

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

Készült Budapesten, 2012. augusztus 29-én, két eredeti példányban, magyar, lett és angol nyelven, mindhárom szöveg egyaránt hiteles. Eltérés esetén az angol nyelvű szöveg az irányadó.

Magyarország Kormánya részéről a Lett Köztársaság Kormánya 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 a 2. § és 3. § 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.

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 Mavtv. 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 a Németországi 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 a 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[1]. Ennek megfelelően hazánk először a 46/2011. (VI. 21.) ME határozat értelmében a Szlovák Köztársasággal, a Lengyel Köztársasággal és a Cseh Köztársasággal kezdte meg a

[1] Egy átlag NATO, EU tagállam a NATO, EU tagállami kört lefedő, és az adott ország külpolitikai és gazdasági orientációjához igazodó kétoldalú titokvédelmi megállapodások széles körével rendelkezik.

tárgyalásokat, melyek közül 2012. május 3-án aláírásra került Budapesten a Szlovák Köztársaság és Magyarország, 2012. június 13-án pedig a Cseh Köztársaság és Magyarország között a minősített adatok cseréjéről és kölcsönös védelméről szóló egyezmény.

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 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. Az Egyezmény 14. Cikk (1) pontja szerint a *„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."*. Ennek oka, hogy az

Egyezmény kötelező hatályának elismerésére a Felek által alkalmazandó alkotmányos vagy belső jogi szabályokkal és eljárásokkal összhangban kerüljön sor. Az Egyezmény hatálybalépésének naptári napját a külpolitikáért felelős miniszter annak ismertté válását követően a Magyar Közlönyben közzétett egyedi közleményével állapítja meg.