Közli: Magyar Közlöny

**2023. évi ... törvény**

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

**1. §**

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

**2. §**

Az Országgyűlés az Egyezményt e törvénnyel kihirdeti.

**3. §**

(1) Az Egyezmény hiteles magyar nyelvű szövegét az 1. melléklet tartalmazza.
(2) Az Egyezmény hiteles angol nyelvű szövegét a 2. melléklet tartalmazza.

**4. §**

(1) Ez a törvény – a (2) bekezdésben foglalt kivétellel – a kihirdetését követő napon lép hatályba.
(2) A 2. §, a 3. §, valamint az 1. melléklet és a 2. melléklet az Egyezmény 15. cikk (1) bekezdésében meghatározott időpontban lép hatályba.
(3) Az Egyezmény, a 2. §, a 3. §, valamint az 1. melléklet és a 2. melléklet hatálybalépésének naptári napját a külpolitikáért felelős miniszter annak ismertté válását követően a Magyar Közlönyben haladéktalanul közzétett közleményével állapítja meg.

**5. §**

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

*1. melléklet a 2023. évi … törvényhez*

# EGYEZMÉNY MAGYARORSZÁG ÉS A SZERB KÖZTÁRSASÁG KÖZÖTT A MINŐSÍTETT ADATOK CSERÉJÉRŐL ÉS KÖLCSÖNÖS VÉDELMÉRŐL

Magyarország és a Szerb Köztársaság (a továbbiakban együtt: a „Felek”)
elismerve a Felek közötti kölcsönös együttműködés jelentőségét,
felismerve, hogy a Felek közötti hatékony együttműködés során szükség lehet minősített adatok cseréjére,
elismerve, hogy azonos szintű védelmet biztosítanak a minősített adatok számára,
kívánatosnak tartva, hogy a közöttük vagy a joghatóságuk alá tartozó jogi személyek és természetes személyek között kicserélt minősített adatok megfelelő védelemben részesüljenek,
kölcsönösen tiszteletben tartva a nemzeti érdekeket és a biztonságot, az alábbiakban állapodtak meg:

## 1. CIKK
## AZ EGYEZMÉNY CÉLJA ÉS TÁRGYA

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

## 2. CIKK
## FOGALOMMEGHATÁROZÁSOK

Jelen Egyezmény alkalmazásában:
a) **minősített adat biztonságának megsértése:** olyan tett vagy mulasztás, amely jelen Egyezménnyel vagy a Felek rájuk vonatkozó saját, nemzeti jogszabályainak és egyéb szabályainak rendelkezéseivel ellentétes, és amely a minősített adat jogosulatlan nyilvánosságra hozatalát, elvesztését, megsemmisülését, jogosulatlan felhasználását, megszerzését vagy bármilyen más típusú megsértését eredményezheti;
b) **minősített szerződés:** olyan szerződés, amely minősített adatot tartalmaz, vagy amely alapján minősített adathoz történő hozzáférés szükséges;
c) **minősített adat**: megjelenési formájától vagy természetétől függetlenül, minden olyan adat, amelyet bármelyik Fél nemzeti jogszabályai és egyéb szabályai szerint védelemben kell részesíteni a minősített adat biztonságának megsértésével szemben, és amelyet ennek megfelelően minősítettek és minősítési szint megjelöléssel láttak el;
d) **szerződést kötő:** az a természetes személy vagy jogi személy, aki a minősített szerződés megkötésére a nemzeti jogszabályok és egyéb szabályok szerint jogképességgel rendelkezik;
e) **telephely biztonsági tanúsítvány:** a nemzeti biztonsági hatóság azon döntése, amely szerint a létesítmény a nemzeti jogszabályokkal és egyéb szabályokkal összhangban rendelkezik a minősített adatok kezelésére és tárolására való fizikai és szervezeti képességgel;
f) **nemzeti biztonsági hatóság:** az állami szerv, amely jelen Egyezmény végrehajtásáért és felügyeletéért felelős;
g) **szükséges ismeret**: az a követelmény, amely alapján minősített adathoz való hozzáférés csak annak a személynek biztosítható, akinek az adott minősített adathoz való hozzáférés hivatali kötelessége vagy meghatározott feladata ellátásához igazoltan szükséges;
h) **átadó Fél:** az a Fél – beleértve a joghatósága alá tartozó jogi személyeket vagy természetes személyeket –, amelyik a minősített adatot átadja;

i) **személyi biztonsági tanúsítvány**: a nemzeti biztonsági hatóság azon döntése, amely megállapítja, hogy egy természetes személy a nemzeti jogszabályokkal és egyéb szabályokkal összhangban hozzáférhet minősített adatokhoz;
j) **átvevő Fél:** az a Fél – beleértve a joghatósága alá tartozó jogi személyeket vagy természetes személyeket –, amelyik a minősített adatot átveszi;
k) **alvállalkozói szerződés:** a szerződést kötő által, egy másik szerződést kötővel (alvállalkozóval) kötött, termékek szolgáltatására vagy szolgáltatások nyújtására irányuló szerződés;
l) **alvállalkozó:** olyan, a minősített szerződések megkötésére irányuló képességgel rendelkező jogi személy vagy természetes személy, akivel a szerződést kötő alvállalkozói szerződést köt;
m) **harmadik fél:** bármely olyan állam – beleértve a joghatósága alá tartozó jogi személyeket vagy természetes személyeket – vagy nemzetközi szervezet, amely nem részese jelen Egyezménynek.

## 3. CIKK
## NEMZETI BIZTONSÁGI HATÓSÁGOK

(1) A Felek nemzeti biztonsági hatóságai a következők:
Magyarországon:
Nemzeti Biztonsági Felügyelet
A Szerb Köztársaságban:
Канцеларија Савета за националну безбедност и заштиту тајних података (Kancelarija Saveta Za Nacionalnu Bezbednost I Zaštitu Tajnih Podataka)
(2) A nemzeti biztonsági hatóságok egymás rendelkezésére bocsátják hivatalos elérhetőségeiket és tájékoztatják egymást a nemzeti biztonsági hatóságokkal kapcsolatos valamennyi későbbi változásról.
(3) A nemzeti biztonsági hatóságok nevében bekövetkező változások nem tekintendőek ezen Egyezmény módosításának. A nemzeti biztonsági hatóságok írásban tájékoztatják egymást e változásokról.

## 4. CIKK
## MINŐSÍTÉSI SZINTEK ÉS MEGFELELŐJÜK

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

| | | |
|---|---|---|
| **Magyarországon** | **A Szerb Köztársaságban** | **Angol nyelvű megfelelőjük** |
| „Szigorúan titkos!” | ДРЖАВНА ТАЈНА | TOP SECRET |
| „Titkos!” | СТРОГО ПОВЕРЉИВО | SECRET |
| „Bizalmas!” | ПОВЕРЉИВО | CONFIDENTIAL |
| „Korlátozott terjesztésű!” | ИНТЕРНО | RESTRICTED |

## 5. CIKK
## MINŐSÍTETT ADATHOZ VALÓ HOZZÁFÉRÉS

Jelen Egyezmény alapján minősített adathoz kizárólag olyan természetes személyek kaphatnak hozzáférést, akik a szükséges ismeret elvének megfelelnek, és a rájuk vonatkozó nemzeti jogszabályoknak és egyéb szabályoknak megfelelően felhatalmazást kaptak a minősített adathoz való hozzáférésre.

## 6. CIKK
## A MINŐSÍTETT ADATOK VÉDELMÉRE VONATKOZÓ ALAPELVEK

(1) Az átadó Fél:
a) biztosítja, hogy a minősített adaton a nemzeti jogszabályai és egyéb szabályai rendelkezéseinek megfelelő minősítési szint feltüntetésre kerüljön;
b) tájékoztatja az átvevő felet a minősített adat felhasználásával kapcsolatos esetleges feltételekről;
c) haladéktalanul írásban tájékoztatja az átvevő felet az adat minősítésében vagy érvényességi idejében bekövetkezett változásokról.
(2) Az átvevő Fél:
a) biztosítja, hogy a minősített adaton feltüntetésre kerüljön a jelen Egyezmény 4. cikke alapján meghatározott egyenértékű minősítési szint;
b) ugyanolyan szintű védelemben részesíti a minősített adatot, mint amelyet a saját, azonos minősítési szintű nemzeti minősített adata számára biztosít;
c) mindaddig biztosítja a minősített adat minősítési szintjének megfelelő védelmet, amíg az átadó Féltől az átvett minősített adat minősítésének megszüntetéséről, illetve minősítési szintjének vagy érvényességi idejének megváltoztatásáról írásban tájékoztatást nem kap;
d) biztosítja, hogy az átadó Fél előzetes írásbeli hozzájárulása nélkül az átvett minősített adatot harmadik fél részére nem adja át;
e) a minősített adatot kizárólag az átadás során megjelölt célra használja fel, betartva az átadó Fél által meghatározott, az adat felhasználásával kapcsolatos átadási feltételeket.

## 7. CIKK
## BIZTONSÁGI EGYÜTTMŰKÖDÉS

(1) Az összeegyeztethető szintű biztonsági követelmények fenntartása érdekében a nemzeti biztonsági hatóságok a másik Fél megkeresésére tájékoztatják egymást a minősített adatok védelmével kapcsolatos nemzeti jogszabályokról és egyéb szabályokról, valamint mindezek gyakorlati alkalmazásáról.
(2) Megkeresés esetén a nemzeti biztonsági hatóságok, összhangban a nemzeti jogszabályaik és egyéb szabályaik rendelkezéseivel, kölcsönösen segítséget nyújtanak egymásnak a személyi biztonsági tanúsítványokkal és a telephely biztonsági tanúsítványokkal kapcsolatos eljárások során.
(3) A Felek megkeresés esetén nemzeti jogszabályaik és egyéb szabályaik rendelkezéseivel összhangban elismerik a másik Fél által kibocsátott személyi biztonsági tanúsítványokat és telephely biztonsági tanúsítványokat. Mindezek során a jelen Egyezmény 4. cikkében foglaltak megfelelően alkalmazandóak.
(4) A nemzeti biztonsági hatóságok haladéktalanul értesítik egymást az elismert személyi biztonsági tanúsítványokkal és telephely biztonsági tanúsítványokkal kapcsolatos változásokról, különösen azok visszavonásáról.
(5) Jelen Egyezmény alapján megvalósuló együttműködés angol nyelven történik.
(6) A Felek titkosszolgálati, biztonsági és rendőri szervei a nemzeti jogszabályaikkal és egyéb szabályaikkal összhangban közvetlenül kicserélhetnek műveleti és/vagy titkosszolgálati információkat, a hatályos, releváns nemzetközi szerződések rendelkezéseivel összhangban.

## 8. CIKK
## MINŐSÍTETT SZERZŐDÉSEK

(1) A minősített szerződéseket a Felek saját nemzeti jogszabályai és egyéb szabályai alapján kell megkötni és teljesíteni. A nemzeti biztonsági hatóságok megkeresésre igazolják, hogy a lehetséges szerződést kötők és a szerződéskötést megelőző tárgyalásokban vagy a minősített szerződések

teljesítésében részt vevők rendelkeznek megfelelő személyi biztonsági tanúsítvánnyal vagy telephely biztonsági tanúsítvánnyal.
(2) A nemzeti biztonsági hatóság kérheti a másik Fél nemzeti biztonsági hatóságától biztonsági ellenőrzés lefolytatását a minősített adatok folyamatos védelmének biztosítása céljából a másik Fél országának területén működő létesítményben.
(3) A minősített szerződések kötelező részét képezi a projekt biztonsági utasítás, amely a biztonsági követelményeket és a szerződés egyes elemeinek minősítésével kapcsolatos rendelkezéseket határozza meg. A projekt biztonsági utasítás másolatát azon Fél nemzeti biztonsági hatósága részére kell továbbítani, amelynek joghatósága alatt a minősített szerződés végrehajtása történik.
(4) Az Átvevő Fél felelős azért, hogy a minősített szerződésekkel kapcsolatban ugyanolyan szabályoknak és követelményeknek megfelelő biztonsági intézkedéseket írjon elő és alkalmazzon, mint amilyet a saját minősített szerződéseinek védelmével kapcsolatban is előír.

## 9. CIKK
## A MINŐSÍTETT ADAT TOVÁBBÍTÁSA

(1) A minősített adat továbbítása az átadó Fél nemzeti jogszabályainak és egyéb szabályainak rendelkezései szerint, diplomáciai úton, vagy a nemzeti biztonsági hatóságok által, írásban közösen meghatározott egyéb módon történik.
(2) A Felek a nemzeti biztonsági hatóságok által írásban jóváhagyott biztonsági eljárási renddel összhangban, elektronikus úton is továbbíthatnak minősített adatot.

## 10. CIKK
## A MINŐSÍTETT ADAT SOKSZOROSÍTÁSA, KIVONATOLÁSA, FORDÍTÁSA ÉS MEGSEMMISÍTÉSE

(1) Jelen Egyezmény alapján átadott minősített adatról készült másolatokon, kivonatokon és fordításokon fel kell tüntetni a megfelelő minősítési szintet és az így készült adatot ugyanolyan védelemben kell részesíteni, mint az eredeti minősített adatot. A sokszorosított példányok számát a hivatalos célból szükséges minimumra kell korlátozni.
(2) Jelen Egyezmény alapján átadott minősített adatról készült fordításokon a fordítás nyelvén fel kell tüntetni, hogy az az átadó Fél minősített adatát tartalmazza.
(3) Jelen Egyezmény alapján átadott „Szigorúan titkos!”/ ДРЖАВНА ТАЈНА / TOP SECRET minősítésű adat sokszorosítása, kivonatolása vagy fordítása kizárólag az Átadó Fél előzetes írásbeli hozzájárulásával történhet.
(4) Jelen Egyezmény alapján átadott „Szigorúan titkos!”/ ДРЖАВНА ТАЈНА / TOP SECRET minősítésű adat nem semmisíthető meg és az átadó Fél részére kell visszaküldeni, ha az átvevő Félnek már nincs szüksége rá.
(5) Olyan válsághelyzet esetén, amely lehetetlenné teszi a minősített adat védelmét vagy visszajuttatását az átadó Félnek, a minősített adatot haladéktalanul meg kell semmisíteni. A minősített adat megsemmisítéséről az átvevő Fél nemzeti biztonsági hatósága haladéktalanul, írásban értesíti az átadó Fél nemzeti biztonsági hatóságát.

## 11. CIKK
## LÁTOGATÁSOK

(1) Minősített adathoz való hozzáférést igénylő látogatásra a fogadó Fél nemzeti biztonsági hatóságának előzetes írásbeli hozzájárulása alapján kerülhet sor.
(2) A látogatást kezdeményező Fél nemzeti biztonsági hatósága a tervezett látogatásról a fogadó Fél nemzeti biztonsági hatóságának legalább húsz nappal a látogatás időpontja előtt látogatási kérelmet

küld. Sürgős esetben, a nemzeti biztonsági hatóságok előzetes egyeztetését követően a 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 intézménynek a megjelölése;
c) a látogató személyi biztonsági tanúsítványának szintje és érvényességi ideje;
d) a látogatás időpontja és időtartama, visszatérő látogatások esetén az egyes látogatások összesített időtartama,
e) a látogatás célja, beleértve a látogatással érintett legmagasabb minősítési szintű minősített adat minősítési szintjét;
f) a meglátogatandó létesítmény neve és címe, valamint a kapcsolattartójának neve, telefonszáma/ fax száma, e-mail címe;
g) dátum, aláírás és a nemzeti biztonsági hatóság hivatalos pecsétjének lenyomata.
(4) A nemzeti biztonsági hatóságok közösen meghatározhatják a visszatérő látogatásra jogosult személyek listáját. A visszatérő látogatások további részleteit a nemzeti biztonsági hatóságok állapítják meg.
(5) A látogató által megismert minősített adatot úgy kell tekinteni, mint a jelen Egyezmény alapján átadott minősített adatot.

## 12. CIKK
## A MINŐSÍTETT ADAT BIZTONSÁGÁNAK MEGSÉRTÉSE

(1) A nemzeti biztonsági hatóságok késedelem nélkül írásban tájékoztatják egymást a minősített adat biztonságának megsértéséről vagy annak gyanújáról.
(2) Annak a Félnek a nemzeti biztonsági hatósága, ahol a minősített adat biztonságának megsértése bekövetkezett, köteles késedelem nélkül gondoskodni az esemény kivizsgálásáról. A másik Fél nemzeti biztonsági hatósága szükség esetén együttműködik a vizsgálatban.
(3) Az átvevő Fél nemzeti biztonsági hatósága minden esetben írásban tájékoztatja az átadó Fél nemzeti biztonsági hatóságát a minősített adat biztonságának megsértésével kapcsolatos körülményekről, a kár mértékéről, a kár enyhítése érdekében megtett intézkedésekről, valamint a vizsgálat eredményéről.

## 13. CIKK
## KÖLTSÉGEK VISELÉSE

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

## 14. CIKK
## MÁS NEMZETKÖZI EGYEZMÉNYEKHEZ VALÓ VISZONY

(1) Jelen Egyezmény semmilyen módon nem befolyásolja azokat a kötelezettségeket, amelyek Magyarország európai uniós tagságából fakadnak. Következésképpen, a jelen Egyezmény rendelkezései nem idézhetőek vagy értelmezhetők úgy, mint amelyek érvénytelenítik, módosítják vagy bármilyen más módon befolyásolják Magyarországnak különösen az Európai Unió alapját képező szerződésekből (az Európai Unióról szóló Szerződésből, az Európai Unió Működéséről szóló Szerződésből, az Európai Atomenergia-közösséget Létrehozó Szerződésből), valamint az Európai Unió elsődleges jogából származó kötelezettségeit.
(2) Jelen Egyezmény nem befolyásolja azokat a kötelezettségeket, amelyek Magyarország NATO tagságából fakadnak. Következésképpen a jelen Egyezmény rendelkezései nem idézhetők vagy értelmezhetők úgy, mint amelyek érvénytelenítik, módosítják vagy bármilyen más módon

befolyásolják Magyarországnak különösen a Washingtonban, 1949. április 4-én létrehozott Észak-atlanti Szerződésből származó kötelezettségeit.
(3) Jelen Egyezmény nem befolyásolja a Felek azon kötelezettségeit, amelyek meglévő két- vagy többoldalú nemzetközi egyezményekből, illetőleg a jelen Egyezmény tárgyával kapcsolatos megállapodásokból erednek.

## 15. CIKK
## ZÁRÓ RENDELKEZÉSEK

(1) Jelen Egyezmény határozatlan időre jön létre. Jelen Egyezmény a Felek által az Egyezmény hatálybalépéséhez szükséges belső jogi feltételek teljesüléséről diplomáciai úton küldött, utolsó értesítés kézhezvételének napját követő második hónap első napján lép hatályba.
(2) Jelen Egyezmény a Felek kölcsönös egyetértésével írásban módosítható. A módosítások hatálybalépésével kapcsolatban a jelen cikk (1) bekezdésében foglaltak az irányadók.
(3) Bármelyik Fél jogosult jelen Egyezményt bármikor írásban felmondani. Felmondás esetén az Egyezmény a felmondásról szóló írásbeli értesítés másik Fél általi kézhezvételének napjától számított hat hónap elteltével hatályát veszti.
(4) Az Egyezmény megszűnésétől függetlenül az annak alapján átadott vagy keletkezett minősített adatokat az Egyezményben meghatározott rendelkezések szerint kell védelemben részesíteni, mindaddig, amíg az átadó Fél írásban felmentést nem ad az átvevő Fél részére ezen kötelezettség alól.
(5) Jelen Egyezmény végrehajtásából vagy értelmezéséből fakadó vitákat a Felek egymás közötti egyeztetés vagy tárgyalás útján, külső igazságszolgáltatási fórum igénybevétele nélkül rendezik.
Fentiek tanúbizonyságául, az alulírott és az erre felhatalmazott megbízottak jelen Egyezményt aláírásukkal látták el.
Készült ……-en, ……..-én, két eredeti példányban, magyar, szerb, és angol nyelven, valamennyi szöveg egyaránt hiteles.
Eltérő értelmezés esetén az angol nyelvű szöveg az irányadó.
……. ……..
Magyarország részéről A Szerb Köztársaság részéről

*2. melléklet a 2023. évi ... törvényhez*

# AGREEMENT BETWEEN HUNGARY AND THE REPUBLIC OF SERBIA ON THE EXCHANGE AND MUTUAL PROTECTION OF CLASSIFIED INFORMATION

Hungary and The Republic of Serbia (hereinafter referred to as the "Parties"),
Recognising the importance of mutual cooperation between the Parties,
Realising that good cooperation may require exchange of classified information between the Parties,
Recognising that they ensure equivalent protection for the classified information,
Wishing to ensure the protection of classified information exchanged between them or between the legal entities or individuals under their jurisdiction,
Have, in mutual respect for national interests and security, agreed upon the following:

## ARTICLE 1
## OBJECTIVE AND APPLICABILITY OF THE AGREEMENT

The objective of this Agreement is to ensure the protection of Classified Information exchanged or generated in the course of co-operation between the Parties or between the legal entities or individuals under their jurisdiction.

## ARTICLE 2
## DEFINITIONS

For the purpose of this Agreement:
a) **"breach of security**" means an act or an omission which is contrary to this Agreement or to the national laws and regulations of the Parties, the result of which may lead to unauthorised disclosure, loss, destruction, misappropriation, access or any other type of compromise of classified information;
b) **"classified contract"** means a contract that involves or requires access to classified information;
c) **"classified information"** means any information that, regardless of its form or nature, under the national laws and regulations of either Party, requires protection against breach of security and has been duly designated;
d) **"contractor**" means an individual or a legal entity possessing the legal capacity to conclude classified contracts in accordance with the national laws and regulations;
e) "**facility security clearance**" means the determination by a national security authority that a facility, possessing the legal capacity, has the physical and organizational capability to handle and store classified information in accordance with the national laws and regulations;
f) "**national security authority**" means the state authority responsible for the application and supervision of this Agreement;
g) **"need-to-know**" means the principle, according to which access to classified information may only be granted to a person who has a verified need to access this classified information in connection with his/her official duties or for the performance of a specific task;
h) **"originating Party"** means the Party including the legal entities or individuals under its jurisdiction, which releases classified information;
i) "**personnel security clearance**" means the determination by a national security authority that an individual is eligible to have access to classified information in accordance with the national laws and regulations;
j) **"recipient Party"** means the Party including the legal entities or individuals under its jurisdiction, which receives classified information;

k) **"sub-contract**" means a contract entered into by a contractor by another contractor (sub-contractor) for a provision of goods and services;
l) "**sub-contractor**" means an individual or a legal entity to whom a contractor lets a sub-contract;
m) **"third party"** means any state including the legal entities or individuals under its jurisdiction or international organisation not being a party to this Agreement.

## ARTICLE 3
## NATIONAL SECURITY AUTHORITIES

(1) The national security authorities of the Parties are:
In Hungary:
Nemzeti Biztonsági Felügyelet (National Security Authority)
In the Republic of Serbia:
Канцеларија Савета за националну безбедност и заштиту тајних података (Office of the National Security Council and Classified Information Protection)
(2) The national security authorities shall provide each other with official contact details and shall inform each other of any subsequent changes regarding the national security authorities.
(3) Changes in the names of the national security authorities shall not constitute modification of this Agreement. The national security authorities shall inform each other in writing about such changes.

## ARTICLE 4
## CLASSIFICATION LEVELS AND MARKINGS

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

| **In Hungary** | **In the Republic of Serbia** | **Equivalent in English** |
|---|---|---|
| „Szigorúan titkos!" | ДРЖАВНА ТАЈНА | TOP SECRET |
| „Titkos!" | СТРОГО ПОВЕРЉИВО | SECRET |
| „Bizalmas!" | ПОВЕРЉИВО | CONFIDENTIAL |
| „Korlátozott terjesztésű!" | ИНТЕРНО | RESTRICTED |

## ARTICLE 5
## ACCESS TO CLASSIFIED INFORMATION

Access to classified information under this Agreement shall be limited only to individuals upon the "need-to-know" principle and who are duly authorised in accordance with the national laws and regulations of the respective Party.

## ARTICLE 6
## SECURITY PRINCIPLES

(1) The originating Party shall:
a) ensure that classified information is marked with appropriate classification markings in accordance with its national laws and regulations;
b) inform the recipient Party of any conditions for using classified information;
c) inform the recipient Party in writing without undue delay of any subsequent changes in the classification level or duration of classification.

(2) The recipient Party shall:
a) ensure that classified information is marked with equivalent classification marking in accordance with Article 4 of this Agreement;
b) afford the same degree of protection to classified information as afforded to its own classified information of equivalent classification level;
c) ensure protection of the classified information equivalent to its classification level until the written notification from the originating Party about the declassification or the change of the classification level or validity of the classified information;
d) ensure that classified information is not released to a third party without the prior written consent of the originating Party;
e) use classified information only for the purpose it has been released for and in accordance with release conditions of the originating Party.

## ARTICLE 7
## SECURITY CO-OPERATION

(1) In order to maintain comparable standards of security, the national security authorities shall, 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 national security authorities shall, in accordance with their national laws and regulations, assist each other during the personnel security clearance procedures and facility security clearance procedures.
(3) On request, the Parties shall in accordance with their national laws and regulations, recognise the personnel security clearances and facility security clearances issued by the other Party. Article 4 of this Agreement shall apply accordingly.
(4) The national security authorities shall promptly notify each other about changes in the recognised personnel security clearances and facility security clearances, especially in case of their withdrawal.
(5) The co-operation under this Agreement shall be effected in the English language.
(6) The intelligence, security and police services of the Parties may directly exchange operational and/or intelligence information in accordance with their national laws and regulations according to the relevant international agreements in force.

## ARTICLE 8
## CLASSIFIED CONTRACTS

(1) Classified contracts shall be concluded and implemented in accordance with the national laws and regulations of each Party. On request, the national security authorities shall confirm that proposed contractors as well as individuals participating in pre-contractual negotiations or in the implementation of classified contracts have appropriate personnel security clearance or facility security clearance.
(2) The national security authority may request its counterpart that a security inspection is carried out at a facility located in the territory of the other Party to ensure continuing protection of classified information.
(3) Classified contracts shall contain project security instructions on the security requirements and on the classification level of each element of the classified contract. A copy of the project security instructions shall be forwarded to the national security authority of the Party under whose jurisdiction the classified contract is to be implemented.
(4) The recipient Party shall assume the responsibility for prescribing and administering security measures for the classified contract under the same standards and requirements that govern the protection of its own classified contracts.

## ARTICLE 9
## TRANSFER OR TRANSMISSION OF CLASSIFIED INFORMATION

(1) Classified information shall be transfered in accordance with the national laws and regulations of the originating Party through diplomatic channels or as otherwise agreed in writing between the national security authorities.
(2) The Parties may transmit classified information by electronic means in accordance with the security procedures approved by the national security authorities in writing.

## ARTICLE 10
## REPRODUCTION, EXTRACTION, TRANSLATION AND DESTRUCTION OF CLASSIFIED INFORMATION

(1) Reproductions, extractions and translations of classified information released under this Agreement shall bear appropriate classification markings and shall be protected as the originals. Number of reproductions shall be limited to that required for official purposes.
(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!"/ ДРЖАВНА ТАЈНА / TOP SECRET shall be reproduced, extracted or translated only upon the prior written consent of the originating Party.
(4) Classified information released under this Agreement marked „Szigorúan titkos!" / ДРЖАВНА ТАЈНА / TOP SECRET shall not be destroyed and shall be returned to the originating Party after it is no longer considered necessary by the recipient Party.
(5) In case of a crisis situation in which it is impossible to protect or to return the classified information to the originating Party it shall be destroyed without undue delay. The national security authority of the recipient Party shall notify the national security authority of the originating Party in writing about the destruction of the classified information.

## ARTICLE 11
## VISITS

(1) Visits requiring access to classified information shall be subject to the prior written consent of the national security authority of the respective Party.
(2) The national security authority of the visiting Party shall notify the national security authority of the host Party about the planned visit through a request for visit at least twenty days before the visit takes place. In urgent cases, the request for visit may be submitted at a shorter notice, subject to prior co-ordination between the national security authorities.
(3) The request for visit shall contain:
a) visitor's name, date and place of birth, nationality and passport/ID card number;
b) position of the visitor and specification of the organisation represented;
c) visitor's personnel security clearance level and its validity;
d) date and duration of the visit, and in case of recurring visits the total period of time covered by the visits;
e) purpose of the visit including the highest classification level of classified information involved;
f) name and address of the facility to be visited, as well as the name, phone/fax number, e-mail address of its point of contact;
g) date, signature and stamping of the official seal of the national security authority.
(4) The national security authorities may agree on a list of visitors entitled to recurring visits. The national security authorities shall agree on the further details of the recurring visits.

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

## ARTICLE 12
## BREACH OF SECURITY

(1) The national security authorities shall without undue delay inform each other in writing of any breach of security or suspicion thereof.
(2) The national security authority of the Party where the breach of security has occurred, shall investigate the incident without undue delay. The national security authority of the other Party shall, if required, co-operate in the investigation.
(3) In any case, the national security authority of the recipient Party shall inform the national security authority of the originating Party in writing about the circumstances of the breach of security, the extent of the damage, the measures adopted for its mitigation and the outcome of the investigation.

## ARTICLE 13
## EXPENSES

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

## ARTICLE 14
## RELATIONSHIP WITH OTHER INTERNATIONAL AGREEMENTS

(1) This Agreement shall in no way prejudice the obligations of Hungary as a member state of the European Union. Consequently the provisions of this Agreement shall not be invoked or interpreted in such a way as to invalidate, modify or otherwise affect the obligations of Hungary imposed especially by the Treaties on which the European Union is founded (the Treaty on European Union, the Treaty on the Functioning of the European Union and the Treaty establishing the European Atomic Energy Community) or by the primary law of the European Union.
(2) This Agreement shall in no way prejudice the obligations of Hungary as a member state of the North Atlantic Treaty Organization. Consequently the provisions of this Agreement shall not be invoked or interpreted in such a way as to invalidate, modify or otherwise affect the obligations of Hungary imposed especially by the North Atlantic Treaty signed in Washington on 4 April 1949.
(3) This Agreement shall not affect the obligations of the Parties under any other bilateral or multilateral treaty, including any agreements governing exchange and mutual protection of Classified Information.

## ARTICLE 15
## FINAL PROVISIONS

(1) This Agreement is concluded for an indefinite period of time. This Agreement shall enter into force on the first day of the second month following the date of receipt of the last of notifications between the Parties, through diplomatic channels, stating that the national legal requirements for this Agreement to enter into force have been fulfilled.
(2) This Agreement may be amended on the basis of the mutual agreement of the Parties in writing. Such amendments shall enter into force in accordance with Paragraph 1 of this Article.
(3) Each Party is entitled to terminate this Agreement in writing at any time. In such a case, the validity of this Agreement shall expire after six months following the day on which the other Party receives the written notice of the termination.

(4) Regardless of the termination of this Agreement, all classified information exchanged or generated under this agreement shall be protected in accordance with the provisions set forth herein until the originating Party dispenses the recipient Party from this obligation in writing.
(5) Any dispute regarding the interpretation or implementation of this Agreement shall be resolved by consultations and negotiations between the Parties, without recourse to outside jurisdiction.
In witness of which, the undersigned, duly authorised to this effect, have signed this Agreement.
Done in …… on …….. in two originals, in the Hungarian, Serbian, and English languages, each text being equally authentic.
In case of different interpretation, the English text shall prevail.
**For Hungary For the Republic of Serbia**