Közli: Magyar Közlöny

2023. évi ... törvény

Magyarország Kormánya és Nagy-Britannia és Észak-Írország Egyesült Királysága Kormánya között a minősített adatok védelméről szóló egyezmény kihirdetéséről

1. §

Az Országgyűlés e törvénnyel felhatalmazást ad Magyarország Kormánya és Nagy-Britannia és Észak-Írország Egyesült Királysága Kormánya között a minősített adatok 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. §, a 6. §, az *1. melléklet* és a *2. melléklet* az Egyezmény 17. cikk (1) bekezdésében meghatározott időpontban lép hatályba.

(3) Az Egyezmény, a 2. §, a 3. §, a 6. §, 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.

6. §

Hatályát veszti a Magyar Köztársaság Kormánya és Nagy-Britannia és Észak-Írország Egyesült Királysága Kormánya között a minősített védelmi információk kölcsönös védelméről szóló, Londonban, 1998. szeptember 7-én aláírt Megállapodás megerősítéséről és kihirdetéséről szóló 1999. évi XIX. törvény.

1. melléklet a 2023. évi….törvényhez

EGYEZMÉNY MAGYARORSZÁG KORMÁNYA ÉS NAGY-BRITANNIA ÉS ÉSZAK-ÍRORSZÁG EGYESÜLT KIRÁLYSÁGA KORMÁNYA KÖZÖTT A MINŐSÍTETT ADATOK VÉDELMÉRŐL

Magyarország és Nagy-Britannia és Észak-Írország Egyesült Királysága ("az Egyesült Királyság") (továbbiakban: „a Felek" vagy egyénileg: "Fél") biztosítani kívánják az általuk létrehozott, közöttük vagy a Magyarországon vagy az Egyesült Királyságban szerződők között kicserélt minősített adatok védelmét, ezért a nemzetbiztonsági érdekek szem előtt tartásával az alábbi egyezményt hozták létre.

1. CIKK
Cél és hatály

(1) Az Egyezmény célja, hogy biztosítsa a Magyarországon vagy az Egyesült Királyságban, vagy együttesen létrehozott, a Felek által egymásnak átadott, az egyik fél és egy szerződő vagy a Felek különböző joghatóságai alatt a nemzeti jogszabályok, egyéb szabályok és szabályzók rendelkezéseinek megfelelően működő szerződők között kicserélt minősített adatok védelmét. Az Egyezmény az e védelemhez szükséges biztonsági eljárásokat és előírásokat állapítja meg.

(2) Az Egyezmény egyetlen rendelkezése sem értelmezhető egyik Fél számára sem kizárólagosan saját minősített adatára vonatkozó kötelező szabályként.

(3) Az Egyezmény egyetlen rendelkezése sem értelmezhető a Felek között minősített adat cseréjére vonatkozó kötelezettségként.

2. CIKK
Fogalmak

A jelen Egyezmény alkalmazásában:

a) **"minősített szerződés":** olyan szerződés vagy szerződéskötést megelőző tárgyalás, amely minősített adatot tartalmaz, vagy amely alapján minősített adathoz történő hozzáférés, minősített adat létrehozása, felhasználása vagy továbbítása szükséges.

b) **"minősített adat":** megjelenési formájától, természetétől vagy továbbítási módjától függetlenül minden olyan adat vagy tárgyi eszköz, amelyet valamely Fél, vagy a közösen létrehozott adat vagy tárgyi eszköz esetén mindkét Fél elhatározása alapján, védelemben kell részesíteni a jogosulatlan hozzáféréssel, nyilvánosságra hozatallal, kezeléssel, felhasználással, elvesztéssel vagy kompromittálódásával szemben.

c) **"hatáskörrel rendelkező biztonsági hatóság" (CSA):** valamely Fél azon kormányzati hatósága, amely jelen Egyezmény rendelkezéseinek végrehajtásáért felelős. A CSA vállalhatja a nemzeti biztonsági hatóság (NSA) bizonyos feladatait is.

d) **"szerződő":** az a természetes vagy jogi személy, amely képességgel rendelkezik minősített szerződések megkötésére, és jelen Egyezmény szerint Félnek nem minősül.

e) **"telephely":** egy létesítmény, üzem, gyár, laboratórium, iroda, egyetem vagy más oktatási intézmény vagy kereskedelmi szervezet (beleértve bármely ezekkel kapcsolatos raktárépületet,

raktárterületet, közművet vagy elemet, melyek funkciójuknál és elhelyezkedésüknél fogva egy működő egységet alkotnak), és bármely állami részleg, ügynökség vagy intézmény.

f) **"telephely biztonsági tanúsítvány" (FSC):** az egyik Fél nemzeti biztonsági hatóságának vagy a hatáskörrel rendelkező biztonsági hatóságának azon döntése, amely szerint a joghatósága alatti szerződő a minősített adat védelmére vonatkozó követelményeket teljesíti, az adott létesítményében rendelkezik azokkal a megfelelő biztonsági feltételekkel, amelyek az adott minősítési szintű minősített adat védelme biztosításához szükségesek a nemzeti jogszabályok, egyéb szabályok és szabályzók rendelkezéseinek megfelelően.

g) **"nemzeti biztonsági hatóság" (NSA):** az egyik Fél azon állami szerve, amely alapvetően felelős a minősített adatok védelméért a jelen Egyezmény és a hatóságra vonatkozó nemzeti jogszabályok, egyéb szabályok és szabályzók rendelkezéseivel összhangban. Az NSA elláthatja a CSA egyes kötelezettségeit is.

h) **"szükséges ismeret":** az a követelmény, amely alapján a minősített adathoz való hozzáférés csak annak a személynek biztosítható, akinek a minősített adathoz való hozzáférés hivatali kötelezettségével összefüggésben vagy meghatározott feladata ellátásához szükséges.

i) **"személyi biztonsági tanúsítvány" (PSC):** a nemzeti biztonsági hatóság vagy a hatáskörrel rendelkező biztonsági hatóság azon döntése, amely szerint egy természetes személy a nemzeti jogszabályok, egyéb szabályok és szabályzók rendelkezéseinek megfelelően felhatalmazással rendelkezik meghatározott minősítési szintű minősített adatokhoz való hozzáféréshez és azok kezeléséhez.

j) **"átadó fél":** az a fél, amelyik jelen Egyezmény alapján a minősített adatot átadja az átvevő félnek.

k) **"átvevő fél":** az a fél, amelyik jelen Egyezmény alapján a minősített adatot átveszi az átadó féltől.

l) **"minősítési szint":** az a kategória, amelyet a Felek a minősített adat szenzitivitásának megjelölésére, valamint a minősített adat jogosulatlan hozzáférhetővé tétele, nyilvánosságra hozatala, kezelése, elvesztése vagy megsértése esetén okozott kár, továbbá a Felek által biztosítandó védelem fokának meghatározására használnak.

m) **"biztonsági esemény"**: olyan, a nemzeti jogszabályok, egyéb szabályok és szabályzók rendelkezéseivel ellentétes tevékenység vagy mulasztás, ami a jelen Egyezmény alapján védelemben részesített minősített adathoz való jogosulatlan hozzáféréshez, nyilvánosságra hozatalhoz, kezeléshez, a minősített adat elvesztéséhez, vagy megsértéséhez vezet.

n) **"harmadik fél":** bármely olyan állam, nemzetközi szervezet, természetes vagy jogi személy (beleértve az államokat és nemzetközi szervezeteket is), amely nem kötelezett jelen Egyezmény előírásainak betartására, és nem alanya minősített szerződésnek.

3. CIKK
Biztonsági hatóságok

(1) A Felek nemzeti biztonsági hatóságai a következők:

Magyarországon	**Az Egyesült Királyságban**

Nemzeti Biztonsági Felügyelet	UK National Security Authority Cabinet Office

(2) A nemzeti biztonsági hatóságok az Egyezmény hatályba lépése után írásban tájékoztatják egymást a hatáskörrel rendelkező biztonsági hatóságokról.

(3) A nemzeti biztonsági hatóságok írásban tájékoztatják egymást a nemzeti biztonsági hatóságokat vagy a hatáskörrel rendelkező biztonsági hatóságokat érintő bármely jelentős változásról.

4. CIKK
Minősítési szintek

(1) A jelen Egyezmény alapján átadott vagy közösen keletkeztetett minősített adatot az átadó fél által a minősítési szintnek megfelelő, egyértelmű, helyesen feltüntetett jelöléssel kell ellátnia, függetlenül attól, hogy az adat papíron jelenik meg, vagy szóbeli, elektronikus, vagy bármely más formában közölt.

(2) A Felek megállapodnak, hogy a minősítési szintek az alábbiak szerint feleltethetők meg egymásnak:

Magyarországon	**Az Egyesült Királyságban**
„Szigorúan titkos!”	UK TOP SECRET
„Titkos!”	UK SECRET
„Bizalmas!”	Nincs egyenértékű (lásd jelen cikk 3. bekezdését)
„Korlátozott terjesztésű!”	UK OFFICIAL-SENSITIVE

(3) Az Egyesült Királyság köteles a „Bizalmas!” minősítési jelöléssel ellátott minősített adatot UK SECRET szintű minősített adatot megillető védelemben részesíteni, kivéve, ha a Felek egybehangzóan másként állapodnak meg.

5. CIKK
Biztonsági alapelvek

(1) A Felek a nemzeti jogszabályaik, egyéb szabályaik és szabályzóik szerint megtesznek minden intézkedést a jelen Egyezmény alapján keletkeztetett és/vagy kicserélt minősített adatok védelme érdekében.

(2) Az átadó fél tájékoztatja az átvevő felet vagy a szerződőt, amely részére minősített adatot ad át, abban az esetben is, ha az átadás szóbeli közléssel történik:

a) az átadott minősített adat minősítési szintjéről és az átadás vagy a felhasználás korlátozásának feltételeiről, és

b) az átadott minősített adat minősítési szintjét érintő minden későbbi változtatásról.

(3) Az átadó fél által az átvevő fél részére történő minősített adat átadása esetén az átvevő fél:

a) ugyanolyan szintű védelemben részesíti a minősített adatot, mint amelyet a saját, azonos minősítési szintű minősített adata számára biztosít (az Egyezmény 4. cikke rendelkezéseinek megfelelően).

b) biztosítja, hogy a minősített adathoz rendelt minősítési jelölés nem kerül megváltoztatásra vagy törlésre, kivéve az átadó fél erre irányuló előzetes írásbeli jóváhagyása esetén.

c) biztosítja, hogy az így átadott minősített adat kizárólag arra célra kerül felhasználásra, amelyre azt átadták (kivéve, ha az átadó fél írásban hozzájárul a további vagy eltérő célú felhasználáshoz), valamint

d) az Egyezmény 7. cikkének és a vonatkozó nemzeti jogszabályoknak, egyéb szabályoknak és szabályzóknak megfelelően biztosítja, hogy az átadó fél előzetes írásbeli hozzájárulása nélkül az átvett minősített adatot harmadik fél részére nem adja át, vagy ilyen adatot nem tesz a nyilvánosság számára hozzáférhetővé.

(4) A jelen cikk (3) bekezdésének c) pontja alapján az átvevő fél számára engedélyezett a minősített adat megosztása annak kormányzati szerveivel, feltéve, ha az átvevő szerv részéről feladatai ellátása céljából szükséges a minősített adathoz történő hozzáférés, és azt az Egyezményben foglalt megfelelő szintű védelemben részesíti.

(5) Az összeegyeztethető szintű biztonsági követelmények fenntartása érdekében a nemzeti biztonsági hatóságok arra irányuló megkeresés esetén megfelelő mértékben tájékoztatják egymást a minősített adatok védelmét érintő biztonsági szabályokról, iránymutatásokról, eljárásokról és gyakorlatokról, valamint ennek érdekében, szükség esetén elősegíthetik a másik Fél képviselői közötti látogatások lebonyolítását.

(6) A nemzeti biztonsági hatóságok tájékoztatják egymást a nemzeti jogszabályaikat, egyéb szabályaikat és szabályzóikat érintő bármely jelentős változásról, amely a jelen Egyezmény hatálya alatt létrehozott és/vagy kicserélt minősített adat védelmét lényegesen érinti.

6. CIKK
Minősített adathoz való hozzáférés

(1) A minősített adatokhoz való hozzáférésre kizárólag azon természetes személyek jogosultak, akik rendelkeznek a szükséges ismerettel, és akiket megfelelően eligazítottak a minősített adat védelmére irányuló felelősségükről és kötelezettségeikről.

(2) „Szigorúan titkos!”, UK TOP SECRET, „Titkos!”, UK SECRET, vagy „Bizalmas!” minősítésű minősített adatokhoz való hozzáférésre az a természetes személy jogosult, aki megfelelő személyi biztonsági tanúsítvánnyal rendelkezik. Kivételes esetben, amennyiben a nemzeti jogszabályok, egyéb szabályok és szabályzók rájuk vonatkozóan ezt megengedik, bizonyos természetes személyek, hivatali feladataik által meghatározottan hozzáférhetnek minősített adatokhoz.

(3) Azon természetes személyek, akik „Szigorúan titkos!” vagy UK TOP SECRET minősítéssel ellátott minősített adatokhoz történő hozzáférésre felhatalmazással rendelkeznek a jelen cikk (2) bekezdésével összhangban, és akik kizárólag magyar vagy brit állampolgárok, vagy kettős állampolgárként magyar és brit állampolgárok, a „Szigorúan titkos!” vagy UK TOP SECRET minősítéssel ellátott minősített adatokhoz az átadó fél előzetes írásbeli hozzájárulása nélkül is hozzáférhetnek. Azon természetes

személyek részére, akik nem az e bekezdésben említett állampolgársággal rendelkeznek, az átadó fél előzetes írásbeli jóváhagyása szükséges.

(4) Azon természetes személyek, akik „Titkos!”, UK SECRET, vagy „Bizalmas!” minősítéssel ellátott minősített adatokhoz történő hozzáférésre felhatalmazással rendelkeznek a jelen cikk (2) bekezdésével összhangban, és akik kizárólag magyar vagy brit állampolgárok vagy kettős állampolgárként magyar és brit állampolgárok, a „Titkos!”, UK SECRET, vagy „Bizalmas!” minősítéssel ellátott minősített adatokhoz az átadó fél előzetes írásbeli hozzájárulása nélkül is hozzáférhetnek. Azon természetes személyek részére, akik nem az e bekezdésben említett állampolgársággal rendelkeznek, az átadó fél előzetes írásbeli jóváhagyása szükséges.

(5) „Korlátozott terjesztésű!” vagy UK OFFICIAL-SENSITIVE minősítéssel ellátott minősített adatokhoz történő hozzáféréshez személyi biztonsági tanúsítvány nem szükséges.

7. CIKK
Minősített adat közzététele

(1) Az átvevő fél a nemzeti jogszabályok, egyéb szabályok és szabályzók alapján megtesz minden olyan szükséges intézkedést, hogy megakadályozza minősített adat nyilvánosságra hozatalát vagy harmadik fél részére történő közzétételét.

(2) A jelen Egyezmény alapján kicserélt minősített adat nyilvánosságra hozatalára vagy harmadik fél részére történő közzétételre vonatkozó kérelem esetén az átvevő fél nemzeti biztonsági hatósága vagy hatáskörrel rendelkező hatósága késedelem nélkül írásban értesíti az átadó fél nemzeti biztonsági hatóságát vagy hatáskörrel rendelkező biztonsági hatóságát, és a Felek írásban egyeztetnek a fogadó fél által a közzétételre vonatkozó döntés meghozatala előtt.

8. CIKK
A minősített adat továbbítása

(1) Ha a fél annak fizikai formájában „Szigorúan titkos!” vagy UK TOP SECRET minősítési szintű minősített adatot kíván továbbítani a minősített adatot átvevő fél területére (vagy az átvevő szerződő területére), azt kormányzati csatornán keresztül kell megvalósítani.

(2) Ha a fél annak fizikai formájában „Titkos!”, UK SECRET vagy „Bizalmas!” minősítési szintű minősített adatot kíván továbbítani a minősített adatot átvevő fél területére (vagy az átvevő szerződő területére), azt kormányzati csatornán keresztül, vagy arra felhatalmazott személyes kézbesítő útján, vagy a nemzeti biztonsági hatóságok vagy a hatáskörrel rendelkező biztonsági hatóságok által közösen, egyetértésben meghatározott módon kell megvalósítani.

(3) Az átvevő fél köteles írásban megerősíteni a „Szigorúan titkos!”, UK TOP SECRET, „Titkos!”, UK SECRET, „Bizalmas!” minősítési szintű adat átvételét. Ennek elősegítése érdekében az átadó fél átvételi bizonylatot csatol a minősített adat mellé, amelyet az átvevő félnek alá kell írnia és egy meghatározott időpontig vissza kell küldenie az átadó félnek.

(4) „Korlátozott terjesztésű!” vagy UK OFFICIAL-SENSITIVE minősítési szintű adat Felek közötti fizikai továbbítása esetén az átadó fél nemzeti jogszabályai, egyéb szabályai és szabályzói alapján kell eljárni.

(5) Ha a fél annak fizikai formájában nagy mennyiségű minősített adatot kíván küldeményként szállítani, elsőként biztosítania kell, hogy a Felek nemzeti biztonsági hatóságai és hatáskörrel rendelkező hatóságai előzetes megállapodásuk eredményeként szállítási tervet dolgoztak ki a szállítási módjáról, az útvonalról és a kíséret feltételeiről. „Korlátozott terjesztésű!" vagy UK OFFICIAL-SENSITIVE minősítési szintű adat szállítása esetén nem szükséges szállítási terv, és a szállítás közvetlenül megszervezhető az átadó és átvevő telephelyek között.

(6) Ha a fél minősített adatot kíván fizikailag továbbítani bármely fél területén kívülre (nem beleértve a fél diplomáciai misszióját), e továbbításhoz az átadó fél előzetes írásbeli jóváhagyása szükséges.

(7) Ha a fél minősített adatot kíván továbbítani elektronikus formában a másik fél részére, azt rejtjelzett formában teheti meg a felek által megállapított kriptográfiai módszerek használatával.

(8) Ha a fél „Korlátozott terjesztésű!" vagy UK OFFICIAL-SENSITIVE minősítési szintű minősített adatot kíván továbbítani elektronikus formában a másik fél részére, azt kivételesen, amennyiben megfelelő kriptográfiai módszerek nem elérhetők és az átadó fél ehhez hozzájárult, nem rejtjelzett formában is megteheti.

(9) A Felek nemzeti biztonsági hatóságai felhatalmazhatják a hatáskörrel rendelkező biztonsági hatóságaikat, hogy minősített adatok kicserélésére vonatkozó alternatív továbbítási módokban állapodjanak meg a jelen Cikkben foglaltak alapján.

9. CIKK

A minősített adat fordítása, sokszorosítása és megsemmisítése

(1) A minősített adatról készült fordításokon és másolatokon az eredeti minősített adat minősítési jelölését kell feltüntetni és az így készült adatot annak megfelelő védelemben kell részesíteni. Az ilyen fordítások vagy sokszorosított példányok számát a hivatalos célhoz szükséges minimumra kell korlátozni, és csak olyan személyek által készíthetők, akik a jelen Egyezmény 6. Cikke alapján hozzáférhetnek minősített adatokhoz.

(2) A jelen Egyezmény alapján átadott minősített adatról készült fordításokon a fordítás nyelvén fel kell tüntetni, hogy az átadó fél minősített adatát tartalmazza.
(3) Olyan minősített adat, amelyre már nincs szükség, az átvevő fél saját, egyező minősítési szintű minősített adatára vonatkozó nemzeti szabályai és módszerei szerint semmisíthető meg.
(4) A minősített adatot olyan válsághelyzet esetén, amely lehetetlenné teszi a védelmét, amint az lehetséges, meg kell semmisíteni oly módon, hogy azt követően az adat jogosulatlan nyilvánosságra hozatala megelőzhető legyen. Minősített adat válsághelyzetben történő megsemmisítéséről az átvevő fél köteles az átadó fél nemzeti biztonsági hatóságát vagy hatáskörrel rendelkező biztonsági hatóságát írásban értesíteni.
(5) Az átadó fél írásbeli értesítés csatolásával, vagy az átvevő félnek kezelési instrukciók biztosításával történő megfelelő jelölés alkalmazásával megtilthatja a minősített adat fordítását, sokszorosítását vagy megsemmisítését.

10. CIKK

Biztonsági együttműködés

(1) A felek nemzeti biztonsági hatósága vagy hatáskörrel rendelkező biztonsági hatóságai, amennyiben szükséges, a nemzeti jogszabályaik, egyéb szabályaik és szabályzóik szerint együttműködnek és segítséget nyújtanak a másik fél nemzeti biztonsági hatóságának vagy hatáskörrel rendelkező

biztonsági hatóságainak a telephely biztonsági tanúsítványok és személyi biztonsági tanúsítványok kiállításával kapcsolatos eljárásaik során.
(2) Amennyiben valamelyik Fél, akár saját nevében, akár egy szerződő nevében telephely biztonsági tanúsítvány kiállítását kérelmezi, vagy megerősítést kér a másik Fél joghatósága alatt működő szerződő telephelyére vonatkozó, meglévő telephely biztonsági tanúsítványát illetően, a nemzeti biztonsági hatóságának vagy hatáskörrel rendelkező biztonsági hatóságának a másik Fél nemzeti biztonsági hatóságához vagy releváns, hatáskörrel rendelkező biztonsági hatóságához legalább az alábbi adatokat tartalmazó írásbeli megkeresést kell benyújtania:
a) A szerződő megnevezése;
b) A szerződő címe;
c) A vonatkozó szerződő fél telephelyének azonosító adatai;
d) A kérelem oka és a telephely biztonsági tanúsítvány szükséges szintje; és
e) A kérelmező nemzeti biztonsági hatóságának vagy hatáskörrel rendelkező biztonsági hatóságának kapcsolattartói adatai (beleértve egy megnevezett személyt és beosztását).
(3) Amennyiben valamelyik Fél, akár saját nevében, akár egy szerződő nevében személyi biztonsági tanúsítvány kiállítását kérelmezi, vagy megerősítést kér egy adott természetes személy részére a másik Fél által kiadni vélt, meglévő személyi biztonsági tanúsítványt illetően, a megerősítést kérő Fél nemzeti biztonsági hatóságának vagy hatáskörrel rendelkező biztonsági hatóságának a másik Fél nemzeti biztonsági hatóságához vagy hatáskörrel rendelkező, releváns biztonsági hatóságához legalább az alábbi adatokat is tartalmazó írásbeli megkeresést kell benyújtania:
a) A természetes személy teljes neve;
b) A természetes személy születési ideje és helye;
c) A természetes személy állampolgársága vagy állampolgárságai;
d) A szervezet vagy szerződő megnevezése, ahol a természetes személy foglalkoztatás alatt áll;
e) A kérelem oka és a személyi biztonsági tanúsítvány szükséges szintje; és
f) A kérelmező nemzeti biztonsági hatóságának vagy hatáskörrel rendelkező biztonsági hatóságának kapcsolattartói adatai (beleértve egy megnevezett személyt és beosztását).
(4) A jelen cikk (2) és (3) bekezdésében foglaltakkal összhangban előterjesztett kérelem beérkezését követően, a kérelmet befogadó nemzeti biztonsági hatóság vagy hatáskörrel rendelkező biztonsági hatóság a kérelmező nemzeti biztonsági hatóság vagy hatáskörrel rendelkező biztonsági hatóság részére rendelkezésre bocsátja az érintett szerződő fél vagy személy vonatkozó telephely biztonsági tanúsítványának vagy személyi biztonsági tanúsítványának adatait, a telephely biztonsági tanúsítvány vagy személyi biztonsági tanúsítvány lejárati dátumát, a minősített adat minősítési szintjét, amelyhez a vonatkozó tanúsítvány hozzáférést, vagy információt biztosít arról, hogy nem áll rendelkezésre érvényes tanúsítvány.
(5) Ha az adott szerződő telephelye nem rendelkezik telephely biztonsági tanúsítvánnyal vagy nem a megfelelő szintű telephely biztonsági tanúsítvánnyal rendelkezik, vagy az adott természetes személy nem rendelkezik személyi biztonsági tanúsítvánnyal vagy nem a megfelelő szintű személyi biztonsági tanúsítvánnyal rendelkezik, akkor a tanúsítvány kiadására irányuló eljárást kell indítani a kérelem teljesítéséhez, a jelen cikk (2) és (3) bekezdésében foglaltak szerint.
(6) A fél nemzeti biztonsági hatósága vagy hatáskörrel rendelkező biztonsági hatósága, megfelelő indok alapján, kérheti a másik fél nemzeti biztonsági hatóságát vagy hatáskörrel rendelkező biztonsági hatóságát, hogy vizsgálja felül az általa kibocsátott telephely biztonsági tanúsítványt és személyi biztonsági tanúsítványt. A felülvizsgálat befejezésekor a felülvizsgálatot végző nemzeti biztonsági hatóság vagy hatáskörrel rendelkező biztonsági hatóság értesíti a kérelmező nemzeti biztonsági hatóságot vagy hatáskörrel rendelkező biztonsági hatóságot az eredményről.
(7) Amennyiben a nemzeti biztonsági hatóság vagy hatáskörrel rendelkező biztonsági hatóság a nemzeti jogszabályaival, egyéb szabályaival és szabályzóival összhangban visszavonja vagy módosítja a szerződő vagy természetes személy telephely biztonsági tanúsítványát vagy személyi biztonsági

tanúsítványát, amelyre a megerősítést korábban megadta, köteles írásban a lehető leghamarabb értesíteni a másik Fél nemzeti biztonsági hatóságát vagy hatáskörrel rendelkező biztonsági hatóságát.

11. CIKK
Minősített szerződések

(1) Ha valamely fél „Szigorúan titkos!”, UK TOP SECRET, „Titkos!”, UK SECRET, vagy „Bizalmas!” minősítési szintű adatot tartalmazó szerződést szándékozik kötni egy másik fél joghatósága alá tartozó szerződővel, a szerződéskötést indítványozó fél nemzeti biztonsági hatóságának vagy hatáskörrel rendelkező biztonsági hatóságának először a másik fél nemzeti biztonsági hatóságától vagy hatáskörrel rendelkező biztonsági hatóságától kell írásbeli megerősítést szereznie a jelen Egyezmény 10. cikkének megfelelően arról, hogy a szerződő és annak releváns alkalmazottai rendelkeznek telephely biztonsági tanúsítvánnyal vagy személyi biztonsági tanúsítvánnyal, legalább a megfelelő minősítési szintig.
(2) Amennyiben megvalósítható, az a nemzeti biztonsági hatóság vagy hatáskörrel rendelkező biztonsági hatóság felelős a szerződő biztonsággal kapcsolatos eljárásának ellenőrzésére, amely a nemzeti jogszabályaik, egyéb szabályaik vagy szabályzóik alapján a vonatkozó telephely biztonsági tanúsítványt vagy személyi biztonsági tanúsítványt kibocsátotta.
(3) Ha a felek közösen nem állapodnak meg másként, a jelen cikk (4) bekezdésére is figyelemmel, a másik fél „Szigorúan titkos!”, UK TOP SECRET, „Titkos!”, UK SECRET, vagy „Bizalmas!”minősítési szintű adatát tartalmazó szerződést megkötő vagy megkötni kívánó félnek meg kell győződnie arról, hogy a szerződő köteles ugyanazon szintű védelemben részesíteni a másik féltől átvett minősített adatot, amilyenben a jelen Egyezmény alapján az átvevő fél azt részesíteni köteles.
(4) A félnek meg kell győződnie arról, hogy a másik fél „Szigorúan titkos!”, UK TOP SECRET, „Titkos!”, UK SECRET, vagy „Bizalmas!” minősítési szintű adatát tartalmazó szerződésnek tartalmaznia kell a következő rendelkezéseket:
a) A jelen Egyezményre történő utalást, a „minősített adat” definícióját a jelen Egyezmény 2. cikke alapján és a Felek egymásnak megfeleltetett minősítési szintjeinek táblázatát a jelen egyezmény 4. cikke alapján.
b) Egy kijelentést, amely szerint a minősített szerződés kapcsán keletkezett és/vagy átadott minősített adatot a hatályos nemzeti jogszabályok, egyéb szabályok és szabályzók szerint kell védeni.
c) A szerződő a másik fél minősített adatát (beleértve azt is, amikor azt a szerződő fél keletkezteti) ugyanolyan módon kezeli, ahogyan azt jelen Egyezmény 5. cikkének (3) bekezdése alapján az átvevő fél kezelni köteles.
d) A jelen Egyezmény 6. cikkének követelményei alapján, a szerződő kizárólag olyan személyek számára biztosítja a minősített adathoz való hozzáférést, akik teljesítik a szükséges ismeret elvének követelményét, a minősített adathoz történő hozzáférésük a nemzeti jogszabályok, egyéb szabályok és szabályzók szerint biztosított, akiket megfelelően eligazítottak a felelősségükről, és akik részére a minősített szerződéssel kapcsolatosan bármilyen feladatot vagy kötelezettséget szabtak ki.
e) A hatályos nemzeti jogszabályok, egyéb szabályok és szabályzók ellenkező rendelkezését kivéve a szerződő nem oszthat meg harmadik féllel vagy nem engedélyezheti a minősített szerződéshez kapcsolódó minősített adat megosztását harmadik féllel, vagy nem teheti azt a nyilvánosság számára hozzáférhetővé, az átadó fél előzetes írásbeli jóváhagyása nélkül.
f) A minősített szerződéshez kapcsolódó minősített adat kizárólag arra a célra használható, amelyre átadták, vagy amelyet később az átadó fél írásban kifejezetten jóváhagyott.
g) A minősített adat továbbítására használandó csatornákra vonatkozó kitétel meghatározása, összhangban jelen Egyezmény 8. cikkével.
h) A minősített adat fordítására, sokszorosítására, és megsemmisítésére vonatkozó kitétel, összhangban jelen Egyezmény 9. cikkével.
i) A szerződőnek tájékoztatnia kell a minősített szerződés ellenőrzéséért felelős nemzeti biztonsági hatóságát vagy hatáskörrel rendelkező biztonsági hatóságát a minősített adat védelmét szolgáló

biztonsági szabályairól, előírásairól, eljárásairól és gyakorlatairól, és e célból elő kell segítenie a minősített szerződés ellenőrzéséért felelős nemzeti biztonsági hatóságának vagy hatáskörrel rendelkező biztonsági hatóságának helyiségeiben történő látogatását.
j) A szerződőtől a másik Fél felelősségi körébe vagy joghatósága alá tartozó telephely látogatásának jóváhagyásával kapcsolatos eljárás részleteit. „Szigorúan titkos!”, UK TOP SECRET, „Titkos!”, UK SECRET, vagy „Bizalmas!”minősítési szintű adathoz történő hozzáférést érintő látogatás esetén a szerződőnek be kell nyújtani a látogatás részleteit a minősített szerződés ellenőrzéséért felelős nemzeti biztonsági hatóságnak vagy hatáskörrel rendelkező biztonsági hatóságnak abból a célból, hogy a nemzeti biztonsági hatóság vagy hatáskörrel rendelkező biztonsági hatóság a látogatási kérelmet a jelen Egyezmény 12. cikke alapján továbbíthassa.
k) A minősített szerződéssel összefüggő, minősített adatok vonatkozásában felmerülő változások (beleértve a minősítési szint megváltozását is) közlésére, vagy az arra vonatkozó eljárások és mechanizmusok részleteit, vagy amikor a védelem már nem szükséges.
l) A szerződő azonnal értesíti a minősített szerződés ellenőrzéséért felelős nemzeti biztonsági hatóságát vagy hatáskörrel rendelkező biztonsági hatóságát bármely feltételezett vagy tényleges biztonsági eseményről a minősített szerződéssel kapcsolatban, és megteszi az összes szükséges lépést a biztonsági esemény hatásainak enyhítése érdekében.
m) Ha a szerződő alvállalkozót vesz igénybe a minősített szerződés egészére vagy részére vonatkozóan, e szerződő alapvetően jelen bekezdés (e pontot is beleértve) rendelkezéseit kell alkalmazza a minősített adathoz történő hozzáférést magában foglaló alvállalkozói szerződésre is.
(5) A „Szigorúan titkos!”, UK TOP SECRET, „Titkos!”, UK SECRET, vagy „Bizalmas!”minősítési szintű minősített adattal kapcsolatos minősített szerződésnek tartalmaznia kell az azt biztosító program biztonsági utasítást és/vagy biztonsági mellékletet, amely meghatározza a biztonsági követelményeket és/vagy a szerződést minősített vonatkozásait.
(6) A fél, amely a „Szigorúan titkos!”, UK TOP SECRET, „Titkos!”, UK SECRET, vagy „Bizalmas!”minősítési szintű minősített adattal kapcsolatos minősített szerződéshez szükséges felhatalmazást adta, köteles a program biztonsági utasítás vagy biztonsági melléklet másolatát a szerződéssel kapcsolatos biztonsági feltételek ellenőrzésének elősegítéséért felelős fél nemzeti biztonsági hatóságának vagy hatáskörrel rendelkező biztonsági hatóságának megküldeni.
(7) A jelen cikk (1), (2), (3), (4), (5) és (6) bekezdése nem alkalmazható „Korlátozott terjesztésű!” vagy UK OFFICIAL-SENSITIVE minősítési szintű adatra korlátozódó minősített szerződések esetében. Az ilyen minősítési szintű minősített adatra korlátozódó minősített szerződéseknek tartalmaznia kell egy megfelelő kikötést, amely az ilyen szintű minősített adat védelmére vonatkozó minimumkövetelményeket meghatározza.

(8) Olyan minősített szerződések esetében, amelyek közösen birtokolt minősített adatot tartalmaznak, a nemzeti biztonsági hatóságok vagy az érintett hatáskörrel rendelkező biztonsági hatóságok egyeztetnek egymással és közösen megállapodnak a szerződésbe foglalandó biztonsági követelményeket tartalmazó kikötésről, a program biztonsági utasításról és/vagy biztonsági mellékletről.

12. CIKK
Látogatások

(1) Ha valamely Fél hivatalos személye a másik Fél joghatósága alá tartozó kormányzati telephelyen látogatást tesz és ez a látogatás „Szigorúan titkos!”, UK TOP SECRET, „Titkos!”, UK SECRET, vagy „Bizalmas!” minősítési szintű minősített adathoz történő hozzáférésével jár vagy járhat, a látogatónak biztosítania kell a minősített adathoz történő hozzáférést biztosító felhatalmazás részleteit a fogadó fél számára a látogatást megelőzően.

(2) Ha valamely fél hivatalos személye a másik fél telephely biztonsági tanúsítvánnyal rendelkező szerződőjének telephelyén látogatást tesz, és ez a látogatás „Szigorúan titkos!”, UK TOP SECRET, „Titkos!”, UK SECRET vagy „Bizalmas!” minősítési szintű minősített adathoz történő hozzáféréssel jár vagy járhat, az eljárás során a jelen cikk (3), (4), (5) és (6) bekezdésében foglaltakat kell követni.

(3) A jelen cikk (2) bekezdésében meghatározott látogatások esetén a látogatási kérelmet a látogatást tervező nemzeti biztonsági hatósága vagy hatáskörrel rendelkező biztonsági hatósága képviselője részére legalább húsz munkanappal a tervezett látogatást megelőzően (vagy nemzeti biztonsági hatóságok vagy az érintett, hatáskörrel rendelkező biztonsági hatóságok megállapodása szerint) kell benyújtania a fogadó telephely nemzeti biztonsági hatóságának vagy hatáskörrel rendelkező biztonsági hatóságának. A látogatási kérelemnek legalább a következő információkat kell tartalmaznia:
a) a látogató teljes neve, születési ideje és helye, állampolgársága, útlevelének (vagy más személyazonosító igazolványának) száma;
b) a látogató hivatalos munkahelyi beosztásának és a látogató által képviselt szervezet megjelölése, illetve ahol alkalmazható, a minősített szerződés vagy program megjelölése, amelyben részt vesznek, és amely a látogatás tárgya;
c) a kérelmezett látogatás vagy látogatások időpontja és időtartama. Visszatérő látogatás esetén a látogatások teljes időtartamát meg kell adni;
d) a látogatás (ok) célja, valamint a tárgyalási téma (témák) megjelölése;
e) a meglátogatandó telephely kapcsolattartójának a neve és címe, telefonszáma/telefaxszáma (ahol alkalmazható), illetve e-mail címe;
f) a megtárgyalandó, megismerendő minősített adat előreláthatható minősítési szintje;
g) a látogató személyi biztonsági tanúsítványa meglétének megerősítése és érvényességi ideje, vagy a minősített adathoz történő hozzáférésére irányuló felhatalmazást igazoló nyilatkozat, a jelen egyezmény 6. cikke (2) bekezdésében foglalt kivétellel összhangban;

h) a látogató nemzeti biztonsági hatósága vagy hatáskörrel rendelkező biztonsági hatósága képviselőjének dátummal ellátott aláírása. A képviselő nem lehet azonos a látogató személyével.

(4) A (3) bekezdésben említett látogatási kérelem több látogatónak az adatait is magában foglalhatja.

(5) A látogatás csak a (jelen cikk (3) bekezdésében meghatározott) látogatási kérelemnek a meglátogatandó telephely nemzeti biztonsági hatósága vagy hatáskörrel rendelkező biztonsági hatósága által történő elfogadása után történhet meg.

(6) Meghatározott minősített szerződések vagy programok esetén a visszatérő látogatók listája létrehozható, mindkét fél nemzeti biztonsági hatóságainak vagy hatáskörrel rendelkező biztonsági hatóságainak előzetes írásbeli jóváhagyásával. Az ilyen listán szereplő megnevezett személyek számára lehetséges, hogy egy meghatározott telephelyet több alkalommal meglátogassanak további írásbeli felhatalmazás nélkül. A lista 12 hónapnál rövidebb ideig érvényes (a jóváhagyás dátumától számítva), és a nemzeti biztonsági hatóságok vagy hatáskörrel rendelkező biztonsági hatóságok jóváhagyása esetén további időszakokra meghosszabbítható. A visszatérő látogatók listáját a jelen cikk (3), (4) és (5) bekezdéseiben foglaltak alapján kell benyújtani és jóváhagyni. Miután a lista engedélyezése megtörtént, a látogatások előkészítése az érintett telephelyek között közvetlenül történik, a nemzeti biztonsági hatóságok vagy hatáskörrel rendelkező biztonsági hatóságok további bevonása nélkül.

(7) A Felek nemzeti biztonsági hatóságai vagy hatáskörrel rendelkező biztonsági hatóságai kölcsönös egyetértésük esetén a jelen cikk (3), (4), (5) és (6) bekezdéseiben foglaltaktól eltérő látogatási eljárást is megállapíthatnak specifikus minősített szerződések vagy programok esetén. Az ilyen alternatív

látogatási eljárásokat a nemzeti biztonsági hatóságoknak vagy az érintett, hatáskörrel rendelkező biztonsági hatóságoknak írásban el kell fogadni és dokumentálni kell.

(8) „Korlátozott terjesztésű!"vagy UK OFFICIAL-SENSITIVE minősített adatot érintő látogatás megszervezése közvetlenül történik a látogató és a meglátogatandó telephely között, a nemzeti biztonsági hatóságok vagy hatáskörrel rendelkező biztonsági hatóságok bevonása nélkül.

13. CIKK
Biztonsági események

(1) Minden feltételezett, a Fél területén vagy egy, a Fél felelőssége alá tartozó telephelyen (beleértve e Fél diplomáciai misszióját is) történt biztonsági eseményt az a Fél köteles kivizsgálni, amelynek területén az megtörtént.

(2) Ha a biztonsági esemény a kivizsgálást folytató Fél által megerősítésre kerül, e Fél köteles megtenni minden megfelelő lépést az esemény következményeinek enyhítése és az ismétlődés elkerülése érdekében a nemzeti jogszabályok, egyéb szabályok és szabályzók szerint.

(3) Amennyiben a biztonsági esemény minősített adat elvesztéséhez vagy kompromittálódásához vezetett, a Fél nemzeti biztonsági hatósága vagy hatáskörrel rendelkező biztonsági hatósága, ahol az esemény történt, vagy azon Fél nemzeti biztonsági hatósága vagy érintett, hatáskörrel rendelkező biztonsági hatósága, amelynek telephelye kapcsán felelősséggel rendelkezik, köteles írásban a lehető leghamarabb értesíteni a másik Fél nemzeti biztonsági hatóságát vagy érintett, hatáskörrel rendelkező biztonsági hatóságát a kivizsgálás kimeneteléről.

14. CIKK
Költségek

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

15. CIKK
Viták rendezése

Bármely Felek közötti, a jelen Egyezmény értelmezését vagy alkalmazását érintő, vagy bármely más, a jelen Egyezményből fakadó vita vagy nézeteltérés esetén a Felek egymás közötti közvetlen tárgyalás útján kötelesek azt rendezni, bármely külső igazságszolgáltatási fórum igénybevétele nélkül.

16. CIKK
Az UK CONFIDENTIAL és UK RESTRICTED minősített adatok védelme

(1) Ha az Egyesült Királyság nem értesítette írásban Magyarországot arról, hogy minősítési szintjét csökkentette vagy a minősítést megszüntette, Magyarország köteles bármely korábbi UK CONFIDENTIAL minősítési szintű minősített adatot a „Bizalmas!" szintű minősített adatot megillető védelemben részesíteni.

(2) Ha az Egyesült Királyság nem értesítette írásban Magyarországot arról, hogy a minősítést megszüntette, Magyarország köteles bármely korábbi UK RESTRICTED minősítési szintű minősített adatot a „Korlátozott terjesztésű!" szintű minősített adatot megillető védelemben részesíteni.

17. CIKK
Záró rendelkezések

(1) A Felek kötelesek egymást diplomáciai úton értesíteni, amint a jelen Egyezmény hatálybalépéséhez szükséges nemzeti intézkedések megtételre kerültek. Az Egyezmény az utolsó értesítés kézhezvételének napját követő második hónap első napján lép hatályba.
(2) A jelen Egyezmény a Felek kölcsönös, írásbeli egyetértésével bármikor módosítható. Az elfogadott módosítások a jelen Cikk 1. pontjában foglaltakkal összhangban lépnek hatályba.
(3) A nemzeti biztonsági hatóságok vagy hatáskörrel rendelkező biztonsági hatóságok a jelen Egyezmény hatálybelépéséhez hatályba léptető rendelkezéseket adhatnak ki.
(4) A jelen Egyezmény a felmondásról szóló értesítésig hatályban marad. Bármelyik Fél jogosult a jelen Egyezményt bármikor, diplomáciai úton, a másik Félnek eljuttatott írásbeli értesítésével megszüntetni, amely a felmondásról szóló írásbeli értesítés másik Fél általi kézhezvételétől számított hat hónap elteltével lép hatályba. Ha az Egyezmény megszűnik, az átadott vagy keletkezett minősített adatokat a minősítés fennállása alatt az Egyezményben meghatározott rendelkezések szerint kell védelemben részesíteni.
(5) A jelen Egyezmény hatályba lépését követően a Fél, amelynek területén a szerződés megkötésre került, haladéktalanul intézkedik az Egyezmény az Egyesült Nemzetek Szervezetének Titkárságánál való bejegyzése iránt, az Egyesült Nemzetek Alapokmányának 102. cikke alapján. A másik Felet értesíteni kell a bejegyzésről és a bejegyzési számról, amint az Egyesült Nemzetek Titkársága kiadta az Egyesült Nemzetek Szerződéstárában.
(6) A Magyar Köztársaság Kormánya és Nagy-Britannia és Észak-Írország Egyesült Királysága Kormánya között a minősített védelmi információk kölcsönös védelméről szóló, 1998. szeptember 7-én aláírt Megállapodás alapján a Felek megállapodnak abban, hogy a Megállapodás hatályát veszti a jelen Egyezmény hatályba lépésével. A korábbi Megállapodás alapján kicserélt vagy keletkezett minősített adatok a jelen Egyezmény rendelkezései szerint védelemben részesülnek.
Fentiek tanúbizonyságául, az alulírott és az erre felhatalmazott megbízottak jelen Egyezményt aláírásukkal látták el.
Készült ……-en, ……..-én két eredeti példányban, magyar és angol nyelven, valamennyi szöveg egyaránt hiteles.

Magyarország Kormánya részéről	Nagy-Britannia és Észak-Írország Egyesült Királysága Kormánya részéről

2. melléklet a 2023. évi ….törvényhez

AGREEMENT BETWEEN THE GOVERNMENT OF THE UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND AND THE GOVERNMENT OF HUNGARY CONCERNING THE PROTECTION OF CLASSIFIED INFORMATION

The United Kingdom of Great Britain and Northern Ireland ("the United Kingdom") and Hungary (referred to jointly as "the Parties" or individually as "a Party"), wishing to ensure the protection of Classified Information generated by the Parties, and/or exchanged between the Parties, or between Contractors in either the United Kingdom or Hungary, have, in the interests of national security, established the following Agreement.

ARTICLE 1
Purpose and scope

1. The purpose of this Agreement is to ensure the protection of United Kingdom, Hungarian, or jointly generated Classified Information, which has been provided by one Party to the other, exchanged between a Party and a Contractor, or between Contractors under the respective Parties' different jurisdictions in accordance with national laws, rules or regulations. This Agreement sets out the security procedures and arrangements for such protection.

2. Nothing in this Agreement shall be interpreted as binding a Party in respect of Classified Information that is exclusively its own.

3. Nothing in this Agreement shall be interpreted as compelling the exchange of Classified Information between the Parties.

ARTICLE 2
Definitions

For the purposes of this Agreement:

a) **"Classified Contract"** means a contract, or pre-contractual negotiations, which contains Classified Information or which involves access to, or the generation, use or transmission of Classified Information.

b) **"Classified Information"** means any information or assets of whatever form, nature or method of transmission determined by a Party, or both Parties for jointly generated information or assets, to require protection against unauthorised access or disclosure, processing, misappropriation, loss or compromise.

c) **"Competent Security Authority"** (CSA) means a Government authority of a Party which is responsible for implementing the provisions set out in this Agreement. A CSA may also undertake some of the responsibilities of a NSA.

d) **"Contractor"** means any natural or legal person with the capacity to enter into Classified Contracts, other than a Party to this Agreement.

e) **"Facility"** means an installation, plant, factory, laboratory, office, university or other educational institution or commercial undertaking (including any associated warehouses, storage areas, utilities and components which, when related by function and location, form an operating entity) and any government department, agency or establishment.

f) **"Facility Security Clearance"** (FSC) means a determination by a NSA or CSA of a Party that a Contractor under its jurisdiction satisfies the conditions for protecting Classified Information and has in place appropriate security measures within a specified Facility to protect Classified Information up to and including a specified Security Classification Level in accordance with its national laws, rules or regulations.

g) **"National Security Authority"** (NSA) means the Government authority of a Party with ultimate responsibility for the security of Classified Information in accordance with the provisions of this Agreement and the national laws, rules or regulations that apply to that authority. A NSA may also undertake some of the responsibilities of a CSA.

h) **"Need to Know"** means the necessity for an individual to have access to Classified Information in connection with official duties and/or for the performance of a specific task.

i) **"Personnel Security Clearance"** (PSC) means a determination by a NSA or CSA that an individual has been authorised to access and handle Classified Information up to and including a specified Security Classification Level in accordance with its national laws, rules or regulations.

j) **"Providing Party"** means the Party that provides Classified Information to the Receiving Party under this Agreement.

k) **"Receiving Party"** means the Party that receives Classified Information from the Providing Party under this Agreement.

l) **"Security Classification Level"** means a category assigned to Classified Information which indicates its sensitivity, the degree of damage that might arise in the event of its unauthorised access or disclosure, misappropriation, loss or compromise, and the level of protection to be applied to it by the Parties.

m) **"Security Incident"** means an act or omission contrary to national laws, rules or regulations, which results in the unauthorised access to, or disclosure, misappropriation, loss, or compromise of Classified Information protected under this Agreement.

n) **"Third Party"** means any State, international organisation, natural or legal person (including States and International Organisations) neither bound to act in accordance with this Agreement nor subject to a Classified Contract.

ARTICLE 3
Security Authorities

1. The NSAs designated by the Parties are:

In the United Kingdom	In Hungary

UK National Security Authority Cabinet Office	Nemzeti Biztonsági Felügyelet

2. Each NSA shall notify the other NSA, in writing, of the relevant CSAs in their country after this Agreement enters into force.

3. Each NSA shall notify the other NSA in writing of any significant changes to their respective NSAs or CSAs.

ARTICLE 4
Security Classification Levels

1. The Security Classification Level of any Classified Information provided, or jointly generated, under this Agreement shall be clearly marked and correctly indicated by the Providing Party, regardless of whether the information is on paper or communicated in oral, electronic or in any other form.

2. The Parties agree that their Security Classification Levels shall correspond to one another as follows:

For the United Kingdom	**For Hungary**
UK TOP SECRET	"Szigorúan titkos!"
UK SECRET	"Titkos!"
No equivalent (see paragraph 3 of this Article)	"Bizalmas!"
UK OFFICIAL-SENSITIVE	"Korlátozott terjesztésű!"

3. Unless otherwise mutually agreed by the Parties, the United Kingdom shall afford Classified Information marked "Bizalmas!" an equivalent level of protection as it would Classified Information at the level of UK SECRET.

ARTICLE 5
Security Measures

1. The Parties shall take all appropriate measures applicable under their national laws, rules or regulations to protect Classified Information generated and/or exchanged under this Agreement.

2. The Providing Party shall ensure that the Receiving Party, or the Contractor to which the Providing Party is providing the Classified Information, including where this is communicated orally, is informed of:

a) the Security Classification Level of the Classified Information provided and any conditions of release or limitations on its use; and

b) any subsequent change in the Security Classification Level of the Classified Information provided.

3. When the Providing Party provides Classified Information to the Receiving Party, the Receiving Party shall:

a) afford such Classified Information the same level of protection as it affords its own Classified Information at the corresponding Security Classification Level (as set out in Article 4 of this Agreement);

b) ensure that the Security Classification Levels assigned to Classified Information are not altered or revoked, except with the prior written approval of the Providing Party;

c) ensure that such Classified Information is used solely for the purpose for which it has been provided (unless the Providing Party approves in writing a further or different purpose); and

d) subject to Article 7 of this Agreement and applicable national laws, rules or regulations, not disclose Classified Information to a Third Party or make such information available to the public without the prior written approval of the Providing Party.

4. Subject to paragraph 3, subsection c) of this Article, the Receiving Party is permitted to share Classified Information internally with other Government organisations of that Party provided that the recipient organisation has a need to access the Classified Information for the purposes of its functions and shall afford it the appropriate level of protection set out in this Agreement.

5. In order to achieve and maintain comparable standards of security, each NSA shall, on request, provide the other NSA with appropriate information about its national security policies, standards, procedures and practices for safeguarding Classified Information, and may for this purpose facilitate such visits by representatives of the other Party as may be deemed appropriate.

6. Each NSA shall notify the other about any significant change to its national laws, rules or regulations that substantially affects the protection of Classified Information generated and/or exchanged under this Agreement.

ARTICLE 6
Access to Classified Information

1. Access to Classified Information shall be limited to individuals who have a Need to Know and who have been appropriately briefed on their responsibilities and obligations to protect Classified Information.

2. Access to Classified Information at the UK TOP SECRET, “Szigorúan titkos!”, UK SECRET, “Titkos!” or “Bizalmas!” levels shall be limited to individuals who have been granted an appropriate PSC. As an exception, certain individuals may be permitted access to Classified Information by virtue of their function if allowed under their respective national laws, rules or regulations.

3. Access to Classified Information at the UK TOP SECRET or “Szigorúan titkos!” level by an individual who has been authorised to access Classified Information to that level in accordance with paragraph 2 of this Article, and holding single British or Hungarian nationality, or dual British and Hungarian nationality, may be granted without the prior written approval of the Providing Party. Access

by individuals not holding the nationalities as set out in this paragraph shall require the prior written approval of the Providing Party.

4. Access to Classified Information at the UK SECRET, “Titkos!” or “Bizalmas!” levels by an individual who has been authorised to access Classified Information at that level, in accordance with paragraph 2 of this Article, and holding either single British or Hungarian nationality, or holding dual nationality where at least one part is British or Hungarian, may be granted without the prior written approval of the Providing Party. Access by individuals not holding the nationalities as set out in this paragraph shall require the prior written approval of the Providing Party.

5. A PSC is not required for access to Classified Information at the UK OFFICIAL-SENSITIVE or “Korlátozott terjesztésű!” level.

ARTICLE 7
Disclosure of Classified Information

1. Within the scope of its national laws, rules or regulations the Receiving Party shall take all reasonable steps to prevent Classified Information being made available to the public or being disclosed to a Third Party.

2. If there is any request or requirement to make Classified Information available to the public or for disclosure to a Third Party, the NSA of the Receiving Party shall immediately notify the NSA of the Providing Party in writing, and both Parties shall consult each other in writing before a disclosure decision is taken by the Receiving Party.

ARTICLE 8
Transmission of Classified Information

1. If a Party wishes to transmit Classified Information at the UK TOP SECRET or “Szigorúan titkos!” level in physical form it shall make arrangements for the Classified Information to be transmitted to the territory of the Receiving Party (or to the territory of the recipient Contractor) through government-to-government channels.

2. If a Party wishes to transmit Classified Information at the UK SECRET, “Titkos!” or “Bizalmas!” level in physical form it shall make arrangements for the Classified Information to be transmitted to the territory of the Receiving Party (or to the territory of the recipient Contractor) through government-to-government channels, by authorised personal hand carriage, or through other means mutually agreed by the NSAs or relevant CSAs.

3. The Receiving Party shall confirm in writing the receipt of Classified Information at the UK TOP SECRET, “Szigorúan titkos!”, UK SECRET, “Titkos!”, or “Bizalmas!” level. To facilitate this, the Providing Party shall include with the Classified Information a receipt for signature by the Receiving Party to be returned to the Providing Party by a specified date.

4. If Classified Information marked UK OFFICIAL-SENSITIVE or “Korlátozott terjesztésű!” is to be transmitted physically between the Parties, it shall be sent in accordance with the national laws, rules or regulations of the Providing Party.

5. If a Party wishes to transport a large volume of Classified Information in physical form as freight it shall first ensure that the means of transport, route and any escort requirements have been mutually

agreed in advance by the NSAs or relevant CSAs of both Parties, and that these are set out in a transportation plan. Transports involving Classified Information at the UK OFFICIAL-SENSITIVE or "Korlátozott terjesztésű!" level do not require transportation plans and can be arranged directly between the sending and receiving Facility.

6. If a Party wishes to transmit Classified Information physically to a final destination outside the territory of either Party (other than to a Party's diplomatic mission) such transmissions shall be subject to the prior written approval of the Providing Party.

7. If a Party wishes to transmit Classified Information electronically to the other Party it shall provide it in encrypted form using cryptographic methods and means mutually accepted by the Parties.

8. If a Party wishes to transmit Classified Information electronically at the UK OFFICIAL-SENSITIVE or "Korlátozott terjesztésű!" level to the other Party it may do so exceptionally in clear text provided suitable cryptographic methods and means are not available and if permitted by the Providing Party.

9. The NSAs of the Parties may permit CSAs of the respective Parties to mutually agree alternative transmission methods to exchange Classified Information to those required by this Article.

ARTICLE 9
Translation, Reproduction and Destruction of Classified Information

1. Translations and reproductions of Classified Information shall retain the security classification marking that was applied to the original and be protected accordingly. Such translations or reproductions shall be limited to the minimum required for an official purpose and shall be made only by individuals who have access to Classified Information in accordance with Article 6 of this Agreement.

2. Translations shall contain a suitable annotation, in the language into which they have been translated, indicating that they contain Classified Information of the Providing Party.

3. When no longer required, Classified Information shall be destroyed in accordance with the standards and methods which the Receiving Party would be required to apply to its own Classified Information at the corresponding Security Classification Level.

4. If a crisis situation makes it impossible to protect Classified Information then it shall be destroyed using any appropriate means as soon as is practicable in order to prevent unauthorised disclosure. The Receiving Party shall notify the NSA or relevant CSA of the Providing Party in writing if Classified Information has been destroyed in a crisis situation.

5. The Providing Party may prohibit the translation, reproduction, or destruction of Classified Information by giving it an appropriate marking, by attaching a written notice or by providing handling instructions to the Receiving Party.

ARTICLE 10
Security Co-operation

1. The NSA and CSAs of a Party shall, where necessary and in accordance with their national laws, rules or regulations, provide assistance and cooperation to the NSA or CSAs of the other Party in the process of issuing FSCs and PSCs.

2. When a Party, whether on behalf of itself or a Contractor, requests the issue of a FSC, or requires confirmation of an existing FSC relating to a Facility of a Contractor under the jurisdiction of the other Party, its NSA or CSA shall submit a formal written request to the NSA or relevant CSA of the other Party, providing at least the following information:

a) Name of the Contractor;

b) Address of the Contractor;

c) Identifying details of the relevant Contractor Facility;

d) Reason for the request and the minimum FSC level required; and

e) Contact details of the requesting NSA or CSA (including a named individual and their position).

3. When a Party, whether on behalf of itself or a Contractor, requests the issue of a PSC or requires confirmation of an existing PSC relating to an individual believed to have been granted by the other Party, the NSA or CSA of the Party requiring confirmation shall submit a formal written request to the NSA or relevant CSA of the other Party, providing at least the following information:

a) Full name of the individual;

b) Date and place of birth of the individual;

c) Nationality or nationalities of the individual;

d) Name of the organisation or Contractor which employs the individual;

e) Reason for the request and the minimum PSC level required; and

f) Contact details of the requesting NSA or CSA (including a named individual and their position).

4. On receipt of a request submitted in accordance with either paragraphs 2 or 3 of this Article, the NSA or CSA receiving the request shall provide the requesting NSA or CSA with details of the relevant FSC or PSC, including the date of expiry of the FSC or PSC, and the Security Classification Level of the Classified Information to which the respective clearance permits access, or provide confirmation that clearance is not held.

5. If a Contractor Facility does not hold a FSC or a FSC at the appropriate level, or an individual does not hold a PSC or a PSC at the appropriate level, the process of initiating a new clearance, as described in paragraphs 2 and 3 of this Article, shall be followed in order to submit the request.

6. A NSA or CSA of a Party may, on providing a valid reason, request the NSA or a CSA of the other Party to undertake a review of any FSC or PSC it has issued. On completion of such a review, the NSA or CSA which undertook the review shall notify the requesting NSA or CSA of the result.

7. If, in accordance with its national laws, rules or regulations, a NSA or CSA withdraws or downgrades a FSC or PSC issued to a Contractor or individual for which or for whom a confirmation has been provided previously, they shall notify the NSA or CSA of the other Party in writing as soon as is practicable.

ARTICLE 11
Classified Contracts

1. If a Party proposes to enter into a Classified Contract involving Classified Information at the UK TOP SECRET, "Szigorúan titkos!", UK SECRET, "Titkos!" or "Bizalmas!" levels with a Contractor under the jurisdiction of the other Party, the NSA or CSA of the Party proposing the contract shall first obtain written confirmation from the NSA or relevant CSA of the other Party, in accordance with Article 10 of this Agreement, that the Contractor and its relevant personnel have been granted a FSC or PSC to at least the appropriate Security Classification Level.

2. The NSA or CSA which has granted a FSC or PSC shall be responsible, where practicable and in accordance with its national laws, rules or regulations, for monitoring the security conduct of the Contractor or individual to which or to whom it applies.

3. Unless mutually agreed by the Parties, and subject to paragraph 4 of this Article, a Party entering or proposing to enter into a Classified Contract involving Classified Information of the other Party at the UK TOP SECRET, "Szigorúan titkos!", UK SECRET, "Titkos!" or "Bizalmas!" levels shall ensure that the Contractor is legally obliged to afford the other Party's Classified Information received at least the same level of protection as the Receiving Party is required to afford it under this Agreement.

4. A Party shall ensure that a Classified Contract involving Classified Information of the other Party at the UK TOP SECRET, "Szigorúan titkos!", UK SECRET, "Titkos!" or "Bizalmas!" levels includes the following provisions:

a) A reference to this Agreement, the definition of the term "Classified Information" as set out in Article 2 of this Agreement, and the table of corresponding Security Classification Levels of the Parties as set out in Article 4 of this Agreement.

b) A statement that Classified Information generated and/or provided as a consequence of the Classified Contract shall be protected in accordance with the applicable national laws, rules or regulations.

c) That the Contractor shall handle the Classified Information of the other Party (including where this is generated by the Contractor) in the same way as a Receiving Party is required to as set out in paragraph 3 of Article 5 of this Agreement.

d) That, in accordance with the requirements of Article 6 of this Agreement, the Contractor shall disclose Classified Information only to individuals who have a Need to Know, have been granted access to Classified Information in accordance with national laws, rules or regulations, have been briefed on their responsibilities, and have been charged with the performance of any tasks or duties in relation to the Classified Contract.

e) That, unless required by applicable national laws, rules or regulations, the Contractor shall not disclose, or permit the disclosure of, Classified Information relating to the Classified Contract to a Third Party or make it available to the public without the prior written approval of the Providing Party.

f) That Classified Information relating to the Classified Contract is to be used solely for the purpose for which it has been provided, or as further expressly approved in writing by the Providing Party.

g) The channels to be used for the transmission of the Classified Information, which shall be in accordance with Article 8 of this Agreement.

h) The procedures for the translation, reproduction and destruction of the Classified Information, which shall be in accordance with Article 9 of this Agreement.

i) That the Contractor shall provide the NSA or CSA responsible for overseeing the Classified Contract with information about its security policies, standards, procedures and practices for safeguarding Classified Information and shall for this purpose facilitate visits to its premises by the representatives of the responsible NSA or CSA.

j) Details of the procedures for the approval of visits by the Contractor to a Facility under the responsibility of the other Party or to a Facility under the jurisdiction of the other Party. Where the visit concerns access to Classified Information at the UK TOP SECRET, "Szigorúan titkos!", UK SECRET, "Titkos!" or "Bizalmas!" levels the Contractor shall be required to submit the details to the NSA or CSA with responsibility for overseeing the Classified Contract in order to enable that NSA or CSA to submit a request for visit in accordance with Article 12 of this Agreement.

k) Details of the procedures and mechanisms for communicating changes that may arise in respect of the Classified Information (including changes in its Security Classification Level) related to the Classified Contract or where protection is no longer necessary.

l) The requirement that the Contractor shall immediately notify its NSA or CSA responsible for overseeing the protection of Classified Information of any actual or suspected Security Incident relating to the Classified Contract and take all reasonable steps to assist in mitigating the effects of such a Security Incident.

m) That should a Contractor sub-contract all or part of the Classified Contract, that Contractor shall include substantially the same provisions as set out in this Article (including this paragraph) in any sub-contract which involves access to Classified Information.

5. Classified Contracts involving Classified Information at the UK TOP SECRET, "Szigorúan titkos!", UK SECRET, "Titkos!" or "Bizalmas!" level shall be supported by a programme security instruction (PSI) and/or security aspects letter (SAL) which identifies the security requirements and/or classified aspects of the contract.

6. The Party awarding or authorising the award of a Classified Contract involving Classified Information at the UK TOP SECRET, "Szigorúan titkos!", UK SECRET, "Titkos!" or "Bizalmas!"

level shall pass a copy the PSI and/or SAL to the NSA or relevant CSA of the Party responsible for facilitating the security monitoring of the contract.

7. Paragraphs 1, 2, 3, 4, 5 and 6 of this Article shall not apply to Classified Contracts that are limited to Classified Information at the UK OFFICIAL-SENSITIVE or "Korlátozott terjesztésű!" level. Classified Contracts that are limited to Classified Information at this Security Classification Level shall contain an appropriate clause identifying the minimum measures to be applied for the protection of such Classified Information.

8. For Classified Contracts involving jointly owned Classified Information, the NSAs or relevant CSAs for the programme shall consult each other and shall mutually agree the provisions of the security requirements clause, and the PSI and/or SAL to be included in the Classified Contract.

ARTICLE 12
Visits

1. If a Government official of a Party is required to visit a Government Facility which is under the jurisdiction of the other Party, and this visit will or may involve access to Classified Information at the UK TOP SECRET, "Szigorúan titkos!", UK SECRET, "Titkos!" or "Bizalmas!" level, the visitor shall ensure that details of their authorisation to access Classified Information are provided to the host Facility prior to the visit.

2. If a Government official of a Party is required to visit a Facility of a Contractor which has been issued a FSC by the other Party, and this visit will or may involve access to Classified Information at the UK TOP SECRET, "Szigorúan titkos!", UK SECRET, "Titkos!" or"Bizalmas!" level, the procedure as set out in paragraphs 3, 4, 5 and 6 of this Article shall be followed.

3. For visits described in paragraph 2 of this Article, a request for visit shall be submitted by a representative of the NSA or relevant CSA of the proposed visitor to the NSA or relevant CSA of the host Facility at least 20 working days in advance of the proposed visit (or as otherwise agreed between the NSAs or relevant CSAs). The request for visit shall include at least the following information:

a) Visitor's full name, date and place of birth, nationality, passport (or other relevant identity document) number;

b) Official job title of the visitor, the name of the organisation they represent and, if applicable, a description of the Classified Contract or programme in which they are participating and which is subject of the visit;

c) Date and duration of the requested visit or visits. In the case of recurring visits the total period covered by the visits shall be stated;

d) Purpose of the visit(s) and subject(s) to be discussed;

e) Name, address, telephone number, fax number (if applicable), and e-mail address of the point of contact of the Facility to be visited;

f) The anticipated Security Classification Level of the Classified Information to be discussed or accessed;

g) Confirmation and date of expiry of the visitor's PSC or a statement confirming their authorisation to access Classified Information in accordance with the exception in paragraph 2 of Article 6 of this Agreement; and

h) A dated signature of a representative of the visitor's NSA or CSA. The representative shall not be the same person as the visitor.

4. A request for visit as referred to in paragraph 3 of this Article may contain the details of multiple visitors.

5. Visits shall only take place when the request for visit (as described in paragraph 3 of this Article) has been authorised by the NSA or relevant CSA of the host Facility.

6. For specific Classified Contracts or programmes it may be possible, subject to the prior written approval of the NSAs or relevant CSAs of both Parties, to establish a recurring visitor list. Such a list allows named individuals to visit a specified Facility more than once without further written authorisation. Such a list shall be valid for a period not exceeding 12 months (from the date of authorisation) and may be extended for further periods of time subject to the approval of the NSAs or relevant CSAs. Recurring visitor lists shall be submitted and approved in accordance with paragraphs 3, 4 and 5 of this Article. Once such a list has been authorised, visit arrangements may be agreed directly by the Facilities involved without the further involvement of the NSAs or CSAs.

7. The NSAs or CSAs of the Parties may mutually determine and agree that alternative visit procedures to paragraphs 3, 4, 5 and 6 of this Article may be adopted for specific Classified Contracts or programmes. Such alternative visit procedures shall be agreed and documented by the NSAs or relevant CSAs in writing.

8. Visits relating to Classified Information at the UK OFFICIAL-SENSITIVE or "Korlátozott terjesztésű!" level shall be arranged directly between the visitor and host Facility to be visited without the involvement of the NSAs or CSAs.

ARTICLE 13
Security Incidents

1. Any suspected Security Incident occurring in the territory of a Party, or at a Facility for which a Party is responsible (including that Party's diplomatic mission), shall be investigated by the Party of the territory where it occurs.

2. If a Security Incident is confirmed by the investigating Party, that Party shall take appropriate measures according to its national laws, rules or regulations to limit the consequences of the incident and prevent recurrence.

3. If a Security Incident has resulted in the loss or compromise of Classified Information the NSA or relevant CSA of the Party in whose territory the incident occurred, or the NSA or relevant CSA of the Facility for which a Party is responsible, shall inform the NSA or CSA of the other Party of the outcome of the investigation in writing as soon as is practicable.

ARTICLE 14
Costs

Each Party shall bear its own costs incurred in the course of implementing its obligations under this Agreement.

ARTICLE 15
Resolution of Disputes

Any dispute or disagreement between the Parties on the interpretation or application of this Agreement, or any other dispute or disagreement arising out of this Agreement, shall be resolved exclusively by means of consultation between the Parties without recourse to any outside jurisdiction.

ARTICLE 16
Protection of legacy UK CONFIDENTIAL and UK RESTRICTED Classified Information

1. Unless the United Kingdom has notified Hungary in writing that it has downgraded or declassified the information, Hungary shall afford any legacy UK CONFIDENTIAL Classified Information it holds the same level of protection it would Classified Information at the "Bizalmas!" level.

2. Unless the United Kingdom has notified Hungary in writing that it has declassified the information Hungary shall afford any legacy UK RESTRICTED Classified Information it holds the same level of protection as it would Classified Information at the "Korlátozott terjesztésű!" level.

ARTICLE 17
Final Provisions

1. Each Party shall notify the other Party through diplomatic channels once the national measures necessary for entry into force of this Agreement have been completed. This Agreement shall enter into force on the first day of the second month following the receipt of the later notification.

2. This Agreement may be amended with the mutual, written consent of the Parties at any time. Agreed amendments shall enter into force in accordance with paragraph 1 of this Article.

3. The NSAs and CSAs may conclude implementing arrangements pursuant to this Agreement.

4. This Agreement shall remain in force until further notice. A Party may terminate this Agreement by written notification delivered to the other Party through diplomatic channels, the termination taking effect six months after such notification is received. If this Agreement is terminated, any Classified Information already provided or generated under this Agreement shall be protected by the Parties in accordance with this Agreement for as long as information remains classified.

5. After the entry into force of this Agreement, the Party in whose territory the Agreement is concluded shall take immediate measures to have this Agreement registered by the Secretariat of the United Nations in accordance with Article 102 of the Charter of the United Nations. The other Party shall be notified of the registration and of the registration number in the UN Treaty Series as soon as the UN Secretariat has issued it.

6. Upon the entry into force of this Agreement, the General Security Arrangement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the Republic of Hungary concerning the mutual protection of classified defence information, dated 7

September 1998 shall be terminated. Any Classified Information generated or exchanged previously under that Arrangement shall be protected in accordance with the provisions of this Agreement.

In witness whereof the duly authorised representatives of the Parties have signed this Agreement,

Done at on the day of , 2023

in two original copies, in the English and Hungarian languages, each text being equally authentic.

For the Government of the United Kingdom of Great Britain and Northern Ireland:	**For the Government of Hungary:**
……	……...