

ACORD

ÎNTRE

ROMÂNIA

ȘI

UNGARIA

PRIVIND PROTECȚIA RECIPROCĂ

A INFORMAȚIILOR CLASIFICATE



România și Ungaria (denumite în continuare „Părți”),

Recunoscând importanța cooperării reciproce între Părți,

Realizând faptul că o bună cooperare poate necesita schimbul de informații clasificate între Părți,

Recunoscând faptul că Părțile asigură același nivel de protecție Informațiilor Clasificate,

Dorind să asigure protecția Informațiilor Clasificate schimbate între Părți sau între persoane juridice ori persoane fizice din statele Părților,

Respectând reciproc interesele naționale și de securitate, au convenit următoarele:

ARTICOLUL 1 DOMENIUL DE APLICARE

1. Prezentul Acord se aplică oricărei activități ce implică schimbul de Informații Clasificate și care se derulează sau urmează a se derula între Părți sau între persoane juridice ori persoane fizice ale Părților.
2. Prezentul Acord nu va afecta obligațiile celor două Părți ce derivă din alte acorduri internaționale cu terți.

ARTICOLUL 2 DEFINIȚII

În scopul prezentului Acord:

- a) **„Incident de Securitate”** înseamnă o acțiune sau omisiune contrară prezentului Acord sau legislațiilor naționale ale Părților care poate avea drept rezultat dezvăluirea, pierderea, distrugerea, însușirea ilegală sau oricare alt tip de compromitere a Informațiilor Clasificate;
- b) **“Contract/Sub-contract Clasificat”** înseamnă orice contract ~~care~~ conține sau necesită acces la Informații Clasificate;



c) **„Informație Clasificată”** înseamnă orice informație care, indiferent de forma sau natura acesteia, necesită protecție și a fost desemnată ca atare, în conformitate cu legislația națională a oricăreia dintre Părți;

d) **„Contractant/Sub-contractant”** înseamnă o persoană juridică abilitată să încheie Contracte/Sub-contracte Clasificate în conformitate cu legislația națională;

e) **„Certificat de Securitate Industrială”** înseamnă un document emis de Autoritatea Națională de Securitate în baza unei proceduri de investigare finalizată printr-o decizie pozitivă, prin care se atestă că o persoană juridică are capacitatea de a proteja informații clasificate în scopul participării la activități pre-contractuale sau să deruleze contracte clasificate, în conformitate cu legislația națională proprie;

f) **„Autoritate Națională de Securitate”** înseamnă autoritatea statului responsabilă de aplicarea și monitorizarea prezentului Acord;

g) **„Necesitatea de a cunoaște”** înseamnă principiul conform căruia accesul la anumite Informații Clasificate poate fi acordat numai acelei persoane îndreptățite să aibă acces la astfel de informații, în virtutea îndatoririlor sale de serviciu sau pentru îndeplinirea unei anumite sarcini;

h) **„Partea Emitentă”** înseamnă Partea, inclusiv persoanele juridice aflate sub jurisdicția acesteia, care generează și transmite Informații Clasificate;

i) **„Certificat de Securitate a Personalului”** înseamnă un document emis în conformitate cu legislația națională aplicabilă, prin care unei persoane i se poate acorda acces la informații de un anumit nivel de clasificare;

j) **„Partea Primitoare”** înseamnă Partea, inclusiv persoanele juridice aflate aflate sub jurisdicția acesteia, care primește Informații Clasificate;

k) **„Tert”** înseamnă orice stat, inclusiv persoane juridice sau persoane fizice aflate sub jurisdicția acestuia, sau organizații internaționale care nu sunt parte la prezentul Acord.



ARTICOLUL 3 AUTORITĂȚILE NAȚIONALE DE SECURITATE

1. Autoritățile Naționale de Securitate ale Părților sunt:

În România:

Oficiul Registrului Național al Informațiilor Secrete de Stat (National Registry Office for Classified Information)

În Ungaria:

Nemzeti Biztonsági Felügyelet (National Security Authority)

2. Autoritățile Naționale de Securitate își vor transmite datele de contact oficiale și se vor informa reciproc cu privire la orice modificări ulterioare ale acestora.

ARTICOLUL 4 NIVELURI DE CLASIFICARE DE SECURITATE ȘI MARCAJE

Echivalența nivelurilor de clasificare de securitate și a marcajelor naționale este următoarea:

În România	În Ungaria	Echivalentul în limba engleză
Strict secret de importanță deosebită	„Szigorúan titkos!”	TOP SECRET
Strict secret	„Titkos!”	SECRET
Secret	„Bizalmas!”	CONFIDENTIAL
Secret de serviciu	„Korlátozott terjesztésű!”	RESTRICTED



ARTICOLUL 5

ACCESUL LA INFORMAȚII CLASIFICATE

Accesul la Informații Clasificate în baza prezentului Acord se va limita numai la persoanele care respectă principiul Necesitatea de a Cunoaște și care au fost autorizate corespunzător în conformitate cu legislația națională a Părții.

ARTICOLUL 6

PRINCIPII DE SECURITATE

1. Partea Emitentă:

- a) se va asigura că Informațiile Clasificate sunt marcate cu marcajele de securitate corespunzătoare, în conformitate cu legislația națională a acesteia;
- b) va informa Partea Primitoare cu privire la orice condiții suplimentare sau limitări în utilizarea Informațiilor Clasificate;
- c) va informa Partea Primitoare, în scris și cu promptitudine, cu privire la orice modificări ulterioare apărute în nivelurile de clasificare de securitate sau la durata clasificării.

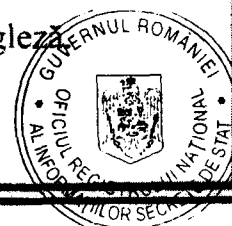
2. Partea Primitoare:

- a) se va asigura că Informațiile Clasificate sunt marcate cu marcajele de clasificare de securitate naționale, în conformitate cu echivalența prevăzută la art. 4;
- b) va acorda același grad de protecție Informațiilor Clasificate cu cel acordat propriilor Informații Clasificate cu nivel de clasificare de securitate echivalent;
- c) se va asigura că Informațiile Clasificate nu sunt declassificate și nici nu li se modifică nivelul de clasificare de securitate fără acordul prealabil scris al Părții Emitente;
- d) se va asigura că Informațiile Clasificate nu sunt transmise unui Terț fără acordul prealabil scris al Părții Emitente;
- e) va utiliza Informațiile Clasificate doar în scopul pentru care au fost transmise și conform condițiilor de transmitere ale Părții Emitente.



ARTICOLUL 7 COOPERAREA DE SECURITATE

1. În scopul menținerii unor standarde comparabile de securitate, la cerere, Autoritățile Naționale de Securitate se vor informa cu privire la legislația națională proprie referitoare la protecția Informațiilor Clasificate și practicile rezultate din implementarea acesteia.
2. La cerere, Autoritățile Naționale de Securitate, în conformitate cu legislațiile naționale proprii, își vor acorda asistență reciprocă pe parcursul procedurii de eliberare a Certificatelor de Securitate a Personalului și a Certificatelor de Securitate Industrială.
3. În sfera de aplicare a prezentului Acord, la cerere, Părțile vor recunoaște Certificatele de Securitate a Personalului și Certificatele de Securitate Industrială emise de cealaltă Parte în conformitate cu legislația națională proprie. Articolul 4 se va aplica în mod corespunzător.
4. Autoritățile Naționale de Securitate se vor informa prompt asupra oricăror modificări intervenite cu privire la Certificatele de Securitate a Personalului și Certificatele de Securitate Industrială recunoscute reciproc, în special în cazul retragerii acestora.
5. Fiecare Parte va informa prompt cealaltă Parte cu privire la orice modificări intervenite în legislația națională care ar putea afecta protecția Informațiilor Clasificate schimbate sau generate în baza prezentului Acord.
6. În cazul Informațiilor Clasificate generate pe parcursul cooperării dintre Părți, atribuirea nivelului de clasificare de securitate, valabilitatea nivelului de clasificare de securitate, modificarea lor sau declasificarea informației respective se va efectua cu acordul Părților, în conformitate cu legislațiile naționale ale acestora.
7. Dacă este cazul, Autoritățile Naționale de Securitate pot încheia aranjamente de securitate pe aspecte tehnice specifice privind implementarea prezentului Acord.
8. Cooperarea în baza prezentului Acord se va desfășura în limba engleză.



ARTICOLUL 8

CONTRACTE CLASIFICATE

1. Contractele Clasificate vor fi încheiate și implementate în conformitate cu legislația națională a fiecăreia dintre Părți. La cerere, Autoritățile Naționale de Securitate vor confirma dacă au fost eliberate Certificate de Securitate a Personalului sau Certificate de Securitate Industrială corespunzătoare Contractanților/Sub-contractanților propuși să participe la negocierile pre-contractuale sau la derularea Contractelor/Sub-contractelor Clasificate anterior accesării de către aceștia a Informațiilor Clasificate ale Părții Emitente.

2. Fiecare Contract/Sub-contract Clasificat încheiat între Contractor/Sub-contractor în conformitate cu prevederile prezentului Acord va cuprinde o anexă de securitate corespunzătoare în care sunt menționate cel puțin următoarele aspecte:

- a) lista Informațiilor Clasificate gestionate în cadrul Contractului/Sub-contractului Clasificat și nivelurile de clasificare de securitate ale acestora;
- b) lista incintelor unde sunt generate sau gestionate Informațiile Clasificate;
- c) procedura de comunicare a modificărilor și valabilității nivelurilor de clasificare de securitate ale informațiilor transmise;
- d) procedura de transport a Informațiilor Clasificate;
- e) obligația de a notifica despre orice Incident de Securitate survenit efectiv sau posibil.

3. Un exemplar al anexe de securitate va fi transmis Autorității Naționale de Securitate a Părții sub jurisdicția căreia urmează să se deruleze Contractul Clasificat.

4. Autoritățile Naționale de Securitate pot conveni asupra unor vizite reciproce în vederea analizării eficienței măsurilor adoptate de Contractant sau de Sub-contractant pentru protecția Informațiilor Clasificate gestionate în Contractul/Sub-contractul Clasificat.



ARTICOLUL 9

TRANSFERUL SAU TRANSMITEREA INFORMAȚIILOR CLASIFICATE

1. Informațiile Clasificate vor fi transferate în conformitate cu legislația națională a Părții Emitente prin canale diplomatice sau prin alte mijloace convenite în scris de Autoritățile Naționale de Securitate, în conformitate cu legislațiile naționale ale acestora.
2. Dacă există un volum mare de Informații Clasificate ce trebuie transferat, Autoritățile Naționale de Securitate vor conveni mijloacele de transport, traseul și măsurile de securitate pentru fiecare caz în parte.
3. Părțile pot transmite Informații Clasificate prin utilizarea mijloacelor electronice în conformitate cu procedurile de securitate aprobate în scris de Autoritățile Naționale de Securitate.
4. Partea Primitoare va confirma în scris primirea Informațiilor Clasificate.

ARTICOLUL 10

MULTIPLICAREA, TRADUCEREA ȘI DISTRUGEREA INFORMAȚIILOR CLASIFICATE

1. Multiplicarea, traducerea și distrugerea Informațiilor Clasificate se vor efectua în conformitate cu legislația națională a Părții Primitoare sau în alt mod convenit între Părți în conformitate cu legislațiile naționale ale acestora.
2. Multiplicările și traducerile Informațiilor Clasificate transmise în baza prezentului Acord vor purta marcaje naționale de clasificare de securitate corespunzătoare, în conformitate cu echivalența prevăzută la art. 4 și vor fi protejate la fel ca și informațiile originale. Numărul copiilor se va limita la cel necesar scopurilor oficiale.
3. Traducerea Informațiilor Clasificate transmise în baza prezentului Acord va conține o notă în limba în care a fost efectuată traducerea în care se va menționa faptul că aceasta cuprinde Informații Clasificate ale Părții Emitente.



4. Informațiile Clasificate transmise în baza prezentului Acord și marcate Strict secret de importanță deosebită/ „Szigorúan titkos!”/ TOP SECRET vor fi traduse sau multiplicare numai cu acordul prealabil scris al Părții Emitente.

5. Informațiile Clasificate transmise în baza prezentului Acord și marcate Strict secret de importanță deosebită/ „Szigorúan titkos!”/ TOP SECRET nu vor fi distruse. Acestea vor fi returnate Părții Emitente după ce Partea Primitoare a considerat că nu mai sunt necesare sau la cererea Părții Emitente.

6. În cazul unei situații de criză în care protejarea sau returnarea Informațiilor Clasificate către Partea Emitentă este imposibilă, acestea vor fi distruse imediat astfel încât reconstrucția parțială sau totală a acestora să nu fie posibilă. Autoritatea Națională de Securitate a Părții Primitoare va informa în scris Autoritatea Națională de Securitate a Părții Emitente cu privire la distrugerea Informațiilor Clasificate.

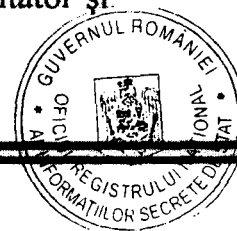
ARTICOLUL 11 VIZITE

1. Vizitele ce implică acces la Informații Clasificate sunt supuse aprobării prealabile scrise a Autorității Naționale de Securitate a Părții corespunzătoare.

2. Autoritatea Națională de Securitate a Părții care efectuează vizita va informa Autoritatea Națională de Securitate a Părții gazdă cu privire la vizita planificată printr-o cerere pentru vizită transmisă cu cel puțin douăzeci de zile înainte ca aceasta să aibă loc. În cazuri de urgență, cererea pentru vizită poate fi înaintată într-un termen mai scurt, în condițiile convenite în prealabil de Autoritățile Naționale de Securitate.

3. Cererea pentru vizită va cuprinde:

- a) numele și prenumele vizitatorului, data și locul nașterii, naționalitatea și numărul pașaportului/cărții de identitate;
- b) funcția vizitatorului și menționarea organizației pe care o reprezintă;
- c) nivelul Certificatului de Securitate a Personalului deținut de vizitator și valabilitatea acestuia;



- d) data și durata vizitei, iar în cazul vizitelor repetate durata totală a acestora;
- e) scopul vizitei, inclusiv cel mai înalt nivel de clasificare de securitate al Informațiilor Clasificate implicate;
- f) denumirea și adresa obiectivului ce urmează a fi vizitat, precum și numele, numărul de telefon și de fax, adresa de email ale punctului de contact;
- g) data, semnătura și ștampila oficială a Autorității Naționale de Securitate.

4. Autoritățile Naționale de Securitate pot conveni asupra unei liste de vizitatori îndreptățiți să efectueze vizite repetate. Autoritățile Naționale de Securitate vor conveni și alte detalii privind vizitele repetate.

5. Informațiile Clasificate de care ia cunoștință un vizitator sunt considerate Informații Clasificate primite în baza prezentului Acord.

ARTICOLUL 12

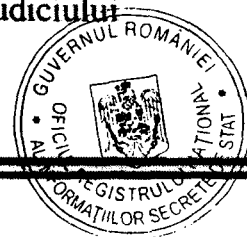
INCIDENT DE SECURITATE

1. Autoritățile Naționale de Securitate se vor informa în scris, cu promptitudine, referitor la producerea oricărui Incident de Securitate sau în cazul în care există indicii despre un astfel de incident.

2. Autoritatea Națională de Securitate din statul Părții unde s-a produs Incidentul de Securitate va investiga imediat incidentul. La cerere, Autoritatea Națională de Securitate a celeilalte Părți va coopera în această investigație.

3. În situația în care Incidentul de Securitate are loc pe teritoriul unui stat terț, Autoritatea Națională de Securitate a Părții trimitătoare va lua toate măsurile necesare pentru a se asigura că au fost inițiate acțiunile prevăzute la alin. (2).

4. În oricare dintre cazuri, Autoritatea Națională de Securitate a Părții Primitoare va informa în scris Autoritatea Națională de Securitate a Părții Emitente cu privire la circumstanțele producerii Incidentului de Securitate, întinderea prejudiciului, măsurile adoptate pentru diminuarea prejudiciului și rezultatul investigației.

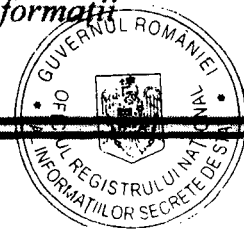


ARTICOLUL 13 CHELTUIELI

Fiecare Parte va suporta cheltuielile proprii generate de implementarea prezentului Acord.

ARTICOLUL 14 DISPOZIȚII FINALE

1. Prezentul Acord se încheie pe o perioadă nedeterminată de timp. Acesta intră în vigoare în prima zi a celei de-a doua luni de la data primirii, prin canale diplomatice, a ultimei notificări între Părți în care se specifică faptul că au fost îndeplinite cerințele naționale legale pentru intrarea în vigoare a prezentului Acord.
2. Prezentul Acord poate fi modificat pe baza consimțământului reciproc, în scris, al Părților. Modificările respective vor intra în vigoare în conformitate cu alin. (1).
3. Fiecare Parte are dreptul să denunțe oricând, în scris, prezentul Acord. În acest caz, valabilitatea Acordului expiră după șase luni de la data la care notificarea de denunțare a fost primită de cealaltă Parte.
4. Chiar și în situația denunțării prezentului Acord, toate Informațiile Clasificate schimbate sau generate în baza acestuia vor continua să fie protejate în conformitate cu prevederile stipulate până când Partea Emitentă dispensează, în scris, Partea Primitoare de această obligație.
5. Orice diferend privind interpretarea sau implementarea prezentului Acord se va soluționa prin consultări și negocieri între Părți fără a se recurge la o altă jurisdicție.
6. La data intrării în vigoare a prezentului Acord se abrogă *Acordul între Guvernul României și Guvernul Republicii Ungare privind protecția reciprocă a schimbului de informații militare secrete de stat, semnat la Debrețin la 17 februarie 1997 și Acordul dintre Guvernul României și Guvernul Republicii Ungare, semnat la Arad la 17 octombrie 2002, privind modificarea art. 1 din Acordul dintre Guvernul României și Guvernul Republicii Ungare privind protecția reciprocă a schimbului de informații militare secrete de stat, semnat la Debrețin la 17 februarie 1997.*



Semnat la **BU CUREȘTI** , la **03 Octombrie 2018** , în două exemplare originale, fiecare în limbile română, maghiară și engleză, toate textele fiind egal autentice. În caz de diferențe de interpretare, textul în limba engleză va prevala.

Drept dovadă subsemnații, pe deplin autorizați, am semnat prezentul Acord.

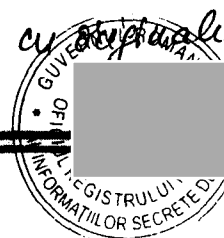
PENTRU ROMÂNIA



PENTRU UNGARIA



Conform cu *[signature]*



EGYEZMÉNY

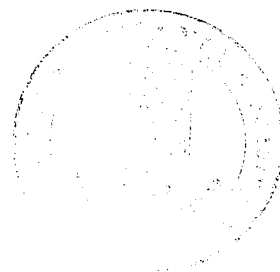
ROMÁNIA

ÉS

MAGYARORSZÁG KÖZÖTT

A MINŐSÍTETT ADATOK

KÖLCSÖNÖS VÉDELMEÉRŐL



Románia és Magyarország (a továbbiakban: Felek)

elismerve a Felek közötti kölcsönös együttműködés jelentőségét,

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

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

kíváncsnak tartva, hogy a Felek között vagy a Felek jogi személyei vagy természetes személyei között kicserélt minősített adatok védelemben részesüljenek,

kölcsönösen tiszteletben tartva a nemzeti érdekeket és a biztonságot, az alábbiakban állapodtak meg:

1. CIKK

AZ EGYEZMÉNY ALKALMAZÁSI TERÜLETE

(1) Jelen Egyezmény alkalmazandó valamennyi, a Felek vagy a Felek jogi személyei vagy természetes személyei között kicserélt vagy kicserélendő minősített adatokkal kapcsolatos tevékenység esetén.

(2) Jelen Egyezmény nem érinti a Felek azon kötelezettségeit, amelyek más, harmadik féllel kötött nemzetközi megállapodások alapján keletkeztek.

2. CIKK

FOGALOMMEGHATÁROZÁSOK

Jelen Egyezmény alkalmazásában:

a) **minősített adat biztonságának megsértése:** olyan, jelen Egyezménnyel vagy a Felek nemzeti szabályozásával ellentétes tevékenység vagy mulasztás, amely a minősített adat nyilvánosságra hozatalához, elvesztéséhez, megsemmisüléséhez, jogosulatlan felhasználásához vagy bármilyen más típusú veszélyeztetéséhez vezethet;

b) **minősített szerződés/alvállalkozói szerződés:** olyan szerződés, amely minősített adatot tartalmaz, vagy amely alapján minősített adathoz való hozzáférés szükséges;

- c) **minősített adat:** megjelenési formájától vagy természetétől függetlenül minden olyan adat, amelyet bármelyik Fél nemzeti szabályozása szerint védelemben kell részesíteni, és amelyet ennek megfelelően minősítettek;
- d) **szerződő/ alvállalkozó:** olyan jogi személy, amely a nemzeti szabályozással összhangban rendelkezik a minősített szerződések/alvállalkozói szerződések megkötésére irányuló képességgel;
- e) **telephely biztonsági tanúsítvány:** a nemzeti biztonsági hatóság által kibocsátott okirat, amely pozitív döntéssel záruló biztonsági ellenőrzés eredményeként született, és a szerződéskötést megelőző tárgyalásokban vagy a minősített szerződés végrehajtásában való részvétel érdekében megállapítja, hogy a jogi személy képes a minősített adatokat a vonatkozó nemzeti szabályozással összhangban védelemben részesíteni;
- f) **nemzeti biztonsági hatóság:** az az állami szerv, amely jelen Egyezmény alkalmazásáért és felügyeletéért felelős;
- g) **szükséges ismeret:** az az elv, amely szerint meghatározott minősített adathoz való hozzáférés kizárólag 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, a joghatósága alá tartozó jogi személyeket beleértve, amely a minősített adatot létrehozza és átadja;
- i) **személyi biztonsági tanúsítvány:** a vonatkozó nemzeti szabályozással összhangban kibocsátott okirat, amely megállapítja, hogy egy természetes személynek bizonyos minősítési szintű adatokhoz való hozzáférés biztosítható;
- j) **átvevő Fél:** az a Fél, a joghatósága alá tartozó jogi személyeket beleértve, amely a minősített adatot átveszi;
- k) **harmadik Fél:** bármely olyan állam, a joghatósága alá tartozó jogi személyeket vagy természetes személyeket beleértve, vagy nemzetközi szervezet, amely nem részese jelen Egyezménynek.

3. CIKK

NEMZETI BIZTONSÁGI HATÓSÁGOK

(1) A Felek nemzeti biztonsági hatóságai:

Romániában:

A minősített adatok nyilvántartásával foglalkozó nemzeti iroda (Oficiul Registrului National al Informatiilor Secrete de Stat, National Registry Office for Classified Information)

Magyarországon:

Nemzeti Biztonsági Felügyelet

(2) A nemzeti biztonsági hatóságok tájékoztatják egymást hivatalos elérhetőségeikről és az azokban bekövetkezett valamennyi későbbi változásról.

4. CIKK

MINŐSÍTÉSI SZINTEK ÉS JELÖLÉSEK

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

Romániában	Magyarországon	Angol nyelvű megfelelőjük
Strict secret de importanță deosebită	„Szigorúan titkos!”	TOP SECRET
Strict secret	„Titkos!”	SECRET
Secret	„Bizalmas!”	CONFIDENTIAL
Secret de serviciu	„Korlátozott terjesztésű!”	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 az érintett Fél nemzeti szabályozásával összhangban erre megfelelő felhatalmazást kaptak.

6. CIKK

BIZTONSÁGI ALAPELVEK

(1) Az átadó Fél:

a) biztosítja, hogy a minősített adaton a nemzeti szabályozása szerinti megfelelő minősítési szint feltüntetésre kerül;

b) tájékoztatja az átvevő Felet a minősített adat felhasználásának esetleges további feltételhez kötéséről vagy korlátozásáról;

c) késedelem nélkül írásban tájékoztatja az átvevő Felet az adat minősítési szintjében vagy a minősítés időtartamában bekövetkezett bármely későbbi változásról.

(2) Az átvevő Fél:

a) biztosítja, hogy a minősített adaton feltüntetésre kerül a jelen Egyezmény 4. cikke alapján meghatározott egyenértékű nemzeti minősítési szint jelölése;

b) ugyanolyan szintű védelemben részesíti a minősített adatot, mint amelyet a saját, egyenértékű minősítési szintű minősített adata számára biztosít;

c) biztosítja, hogy az átadó Fél előzetes írásbeli hozzájárulása nélkül a minősített adat minősítése nem kerül megszüntetésre, valamint minősítési szintje nem kerül megváltoztatásra;

d) biztosítja, hogy az átadó Fél előzetes írásbeli hozzájárulása nélkül a 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 átadási feltételeket.

7. CIKK

BIZTONSÁGI EGYÜTTMŰKÖDÉS

(1) Az összeegyeztethető szintű biztonsági követelmények fenntartása érdekében a nemzeti biztonsági hatóságok megkeresésre tájékoztatják egymást a minősített adat védelmével kapcsolatos nemzeti szabályozásukról, valamint annak gyakorlati alkalmazásáról.

(2) Megkeresés esetén a nemzeti biztonsági hatóságok nemzeti szabályozásukkal összhangban segítséget nyújtanak egymásnak a személyi biztonsági tanúsítványokkal és telephely biztonsági tanúsítványokkal kapcsolatos eljárások során.

(3) Jelen Egyezmény keretében a Felek megkeresés esetén elismerik a másik Fél által, annak nemzeti szabályozásával összhangban kibocsátott személyi biztonsági tanúsítványokat és telephely biztonsági tanúsítványokat. A 4. cikkben foglaltak megfelelően alkalmazandók.

(4) A nemzeti biztonsági hatóságok haladéktalanul értesítik egymást az elismert személyi biztonsági tanúsítványokkal és telephely biztonsági tanúsítványokkal kapcsolatos változásokról, különösen azok visszavonásáról.

(5) A Felek haladéktalanul értesítik egymást a nemzeti szabályozásukban bekövetkezett valamennyi olyan változásról, amely érintheti a jelen Egyezmény alapján kicserélt vagy keletkezett minősített adat védelmét.

(6) A Felek közötti együttműködés keretében létrejött minősített adat esetében a minősítés szintjének meghatározása, a minősítés időtartamának meghatározása, ezek megváltoztatása vagy a minősítés megszüntetése a Felek közötti egyetértéssel és nemzeti szabályozásukkal összhangban történik.

(7) Szükség esetén a nemzeti biztonsági hatóságok jelen Egyezmény végrehajtása céljából meghatározott technikai kérdéseket érintő biztonsági megállapodásokat köthetnek.

(8) A jelen Egyezmény alapján megvalósuló együttműködés angol nyelven történik.

8. CIKK

MINŐSÍTETT SZERZŐDÉSEK

(1) A minősített szerződéseket a Felek nemzeti szabályozásával összhangban kell megkötni és teljesíteni. A nemzeti biztonsági hatóságok megkeresésre még azt megelőzően megerősítik, hogy a szerződéskötést megelőző tárgyalásokban vagy a minősített szerződések/alvállalkozói szerződések teljesítésében részt vevő szerződők/alvállalkozók rendelkeznek megfelelő személyi biztonsági tanúsítvánnyal vagy telephely biztonsági tanúsítvánnyal, hogy azok az átadó Fél minősített adatához hozzáférhessenek.

(2) A jelen Egyezmény alapján a szerződők/alvállalkozók között kötött minősített szerződésnek/alvállalkozói szerződésnek olyan biztonsági mellékletet is tartalmaznia kell, amelyben legalább az alábbiak szerepelnek:

- a) a minősített szerződéssel/alvállalkozói szerződéssel érintett minősített adatok és azok minősítési szintjének listája;
- b) azon épületek listája, ahol minősített adatot hoznak létre vagy kezelnek;
- c) a változásokról és az átadott adatok minősítési szintjének érvényességéről történő tájékoztatásra vonatkozó eljárás;
- d) a minősített adat szállításának menete;
- e) értesítési kötelezettség a minősített adat biztonságának tényleges vagy feltételezett megsértése esetén.

(3) A biztonsági melléklet másolatát meg kell küldeni azon Fél nemzeti biztonsági hatóságának, amelynek joghatósága alatt a minősített szerződés teljesítése történik.

(4) A nemzeti biztonsági hatóságok megállapodhatnak kölcsönös látogatások lefolytatásáról a szerződő/alvállalkozó által a szerződéssel/alvállalkozói szerződéssel érintett minősített adatok védelme érdekében hozott intézkedések hatékonyságának ellenőrzése céljából.

9. CIKK

A MINŐSÍTETT ADAT TOVÁBBÍTÁSA

- (1) A minősített adat továbbítása az átadó Fél nemzeti szabályozásával összhangban, diplomáciai úton vagy a Felek nemzeti szabályozásával összhangban, a nemzeti biztonsági hatóságok által írásban meghatározott egyéb módon történik.
- (2) Minősített adatot tartalmazó nagyméretű küldemény továbbítása esetén a nemzeti biztonsági hatóságok eseti jelleggel rendelkeznek a szállítás módjáról, az útvonalról és a biztonsági intézkedésekről.
- (3) A Felek a nemzeti biztonsági hatóságok által írásban jóváhagyott biztonsági eljárási renddel összhangban elektronikus úton is továbbíthatnak minősített adatot.
- (4) Az átvevő Fél a minősített adat átvételét írásban visszaigazolja.

10. CIKK

A MINŐSÍTETT ADAT SOKSZOROSÍTÁSA, FORDÍTÁSA ÉS MEGSEMMISÍTÉSE

- (1) A minősített adat sokszorosítása, fordítása és megsemmisítése az átvevő Fél nemzeti szabályozásával összhangban vagy a Felek nemzeti szabályozásával összhangban álló, általuk meghatározott egyéb módon történik.
- (2) Jelen Egyezmény alapján átadott minősített adatról készült sokszorosított példányokon és fordításokon fel kell tüntetni a megfelelő nemzeti minősítési jelölést a 4. cikkben foglalt megfeleltetéssel összhangban, és az így készült adatot ugyanolyan védelemben kell részesíteni, mint az eredeti minősített adatot. A sokszorosított példányok számát a hivatalos célból szükséges mértékre kell korlátozni.
- (3) A jelen Egyezmény alapján átadott minősített adat fordításán a fordítás nyelvén fel kell tüntetni, hogy az az átadó Fél minősített adatát tartalmazza.
- (4) A jelen Egyezmény alapján átadott Strict secret de importanță deosebită / „Szigorúan titkos!” / TOP SECRET minősítési jelölésű adat fordítása vagy sokszorosítása kizárólag az átadó Fél előzetes írásbeli hozzájárulásával lehetséges.
- (5) A jelen Egyezmény alapján átadott Strict secret de importanță deosebită / „Szigorúan titkos!” / TOP SECRET minősítési jelölésű adat nem semmisíthető meg. Azokat az átadó Félnak vissza kell szolgáltatni, miután az átvevő Félnak azokra már nincs szüksége, vagy az átadó Fél kérelme esetén.

(6) Olyan válsághelyzet esetén, amely lehetetlenné teszi a minősített adat védelmét vagy az átadó Félhez való visszajuttatását, a minősített adatot késedelem nélkül meg kell semmisíteni oly módon, hogy a helyreállítása sem részben, sem egészben ne legyen lehetséges. A minősített adat megsemmisítéséről az átvevő Fél nemzeti biztonsági hatósága írásban értesíti az átadó Fél nemzeti biztonsági hatóságát.

11. CIKK LÁTOGATÁSOK

(1) Minősített adathoz való hozzáférést igénylő látogatásra az érintett Fél nemzeti biztonsági hatóságának előzetes írásbeli jóváhagyása 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 megkeresést 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 tartalmaznia kell az alábbiakat:

- a) a látogató neve, születési helye és ideje, állampolgársága, útlevelének vagy más személyazonosító igazolványának száma;
- b) a látogató beosztása és a látogató által képviselt szervezet meghatározása;
- 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 szintjének megjelölését;
- f) a meglátogatandó létesítmény neve és címe, valamint a kapcsolattartójának neve, telefonszáma, faxszáma, 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 nemzeti biztonsági hatóságok megállapodnak a visszatérő látogatások további részleteiről.

(5) A látogató által megismert minősített adatot úgy kell tekinteni, mint a jelen Egyezmény alapján átvett 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) Azon Fél nemzeti biztonsági hatósága, ahol a minősített adat biztonságának megsértése bekövetkezett, késedelem nélkül kivizsgálja az esetet. A másik Fél nemzeti biztonsági hatósága szükség esetén közreműködik a vizsgálatban.
- (3) Ha a minősített adat biztonságának megsértése harmadik állam területén következik be, a kézbesítő Fél nemzeti biztonsági hatósága köteles megtenni a szükséges intézkedéseket a (2) bekezdésben szereplő intézkedések megkezdésének biztosítása érdekében.
- (4) Az átvevő Fél nemzeti biztonsági hatósága minden esetben írásban tájékoztatja az átadó Fél nemzeti biztonsági hatóságát a minősített adat biztonsága megsértésének körülményeiről, a kár mértékéről, a kár enyhítése érdekében megtett intézkedésekről, valamint a vizsgálat eredményéről.

13. CIKK

KÖLTSÉGEK

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

14. CIKK

ZÁRÓ RENDELKEZÉSEK

- (1) Jelen Egyezmény határozatlan időre jön létre. Jelen Egyezmény a Felek által az Egyezmény hatálybalépéshez szükséges nemzeti 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 az (1) bekezdésben foglaltak az irányadók.
- (3) Bármelyik Fél jogosult jelen Egyezményt bármikor írásban felmondani. Felmondás esetén az Egyezmény a felmondásról szóló írásbeli értesítés másik Fél általi kézhezvételétől számított hat hónap elteltével hatályát veszti.

(4) Az Egyezmény megszűnésétől függetlenül a jelen Egyezmény alapján kicserélt vagy keletkezett valamennyi minősített adatot az Egyezményben meghatározott rendelkezések szerint kell védelemben részesíteni mindaddig, amíg az átadó Fél írásban felmentést nem ad az átvevő Fél részére e kötelezettség alól.

(5) A jelen Egyezmény értelmezéséből vagy végrehajtásából fakadó vitákat a Felek egymás között egyeztetés és tárgyalás útján, külső igazságszolgáltatási fórum igénybevétele nélkül rendezik.

(6) Jelen Egyezmény hatálybalépésével megszűnik a Románia Kormánya és a Magyar Köztársaság Kormánya között a minősített katonai információk kölcsönös védelme tárgyában Debrecenben, 1997. február 17-én aláírt Egyezmény, valamint a Románia Kormánya és a Magyar Köztársaság Kormánya között a minősített katonai információk kölcsönös védelme tárgyában aláírt Egyezmény 1. cikkének módosításáról szóló, Aradon, 2002. október 17-én aláírt Megállapodás.

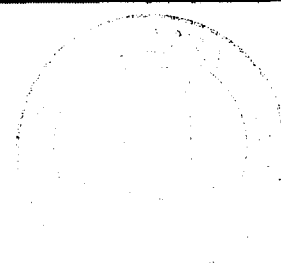
Készült Bukarestben, 2018. 10. 03 -án, két eredeti példányban, román, magyar és angol nyelven, valamennyi szöveg egyaránt hiteles. Eltérő értelmezés esetén az angol nyelvű szöveg az irányadó.

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

ROMÁNIA RÉSZÉRŐL



MAGYARORSZÁG RÉSZÉRŐL



AGREEMENT

BETWEEN

ROMANIA

AND

HUNGARY

ON MUTUAL PROTECTION

OF CLASSIFIED INFORMATION

Romania and Hungary (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 of the Parties,

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

ARTICLE 1 APPLICABILITY

1. This Agreement is applicable to any activity involving the exchange of Classified Information, conducted or to be conducted between the Parties or between legal entities or individuals of the Parties.
2. This Agreement shall not affect the commitments of both Parties which stem from other international agreements with third parties.

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 legislations of the Parties, the result of which may lead to disclosure, loss, destruction, misappropriation or any other type of compromise of Classified Information;
- b) **"Classified Contract/Sub-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 legislation of either Party, requires protection and has been duly designated;

d) **"Contractor/Sub-contractor"** means a legal entity possessing the legal capacity to conclude Classified Contracts/Sub-contracts in accordance with the national legislation;

e) **"Facility Security Clearance Certificate"** means a document issued by the National Security Authority and stemming from an investigative procedure finalized with a positive decision which determines the capability of a legal entity to protect classified information in order to participate in pre-contractual activities or perform classified contracts, in accordance with the respective national legislation;

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 specific 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 legal entities under its jurisdiction, which originates and releases Classified Information;

i) **"Personnel Security Clearance Certificate"** means a document issued in accordance with the respective national legislation determining that access to information of a certain security classification level may be granted to an individual;

j) **"Recipient Party"** means the Party including legal entities under its jurisdiction, which receives Classified Information;

k) **"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 Romania:

Oficiul Registrului Național al Informațiilor Secrete de Stat (National Registry Office for Classified Information)

In Hungary:

Nemzeti Biztonsági Felügyelet (National Security Authority)

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

ARTICLE 4
SECURITY CLASSIFICATION LEVELS AND MARKINGS

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

In Romania	In Hungary	Equivalent in English language
Strict secret de importanță deosebită	„Szigorúan titkos!”	TOP SECRET
Strict secret	„Titkos!”	SECRET
Secret	„Bizalmas!”	CONFIDENTIAL
Secret de serviciu	„Korlátozott terjesztésű!”	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 legislation of the respective Party.

ARTICLE 6
SECURITY PRINCIPLES

1. The Originating Party shall:

- a) ensure that Classified Information is marked with appropriate security classification markings in accordance with its national legislation;
- b) inform the Recipient Party of any additional conditions or limitations on use of Classified Information;
- c) inform the Recipient Party in writing without undue delay of any subsequent changes in the security classification level or duration of classification.

2. The Recipient Party shall:

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

ARTICLE 7
SECURITY COOPERATION

1. In order to maintain comparable standards of security, the National Security Authorities shall, on request, inform each other of their national legislation concerning the protection of Classified Information and the practices stemming from their implementation.

2. On request, the National Security Authorities shall, in accordance with their national legislation, assist each other during the personnel security clearance procedures and facility security clearance procedures.

3. Within the scope of this Agreement, on request, the Parties shall recognise the Personnel Security Clearance Certificates and Facility Security Clearance Certificates issued by the other Party in accordance with its national legislation. Article 4 shall apply accordingly.

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

5. Each Party shall promptly notify the other Party of any amendments to its national legislation that would affect the protection of Classified Information exchanged or generated under this Agreement.

6. When classified information is generated in the course of cooperation between the Parties, the assignment of a security classification level, the validity of the security classification level, their change or the declassification shall be made upon common consent of the Parties, in accordance with their national legislation.

7. If the need arises, the National Security Authorities may conclude security arrangements on specific technical aspects concerning the implementation of this Agreement.

8. The cooperation under this Agreement shall be effected in the English language.

ARTICLE 8

CLASSIFIED CONTRACTS

1. Classified Contracts shall be concluded and implemented in accordance with the national legislation of each Party. On request, the National Security Authorities shall confirm that proposed Contractors/Sub-contractors participating in pre-contractual negotiations or in the implementation of Classified Contracts/Sub-contracts have been issued appropriate Personnel Security Clearance Certificates or Facility Security Clearance Certificates, before accessing Classified Information of the Originating Party.

2. Every Classified Contract/Sub-contract concluded between Contractors/Sub-contractors, under the provisions of this Agreement, shall include an appropriate security annex identifying at least the following aspects:

- a) a list of Classified Information related to the Classified Contract/Sub-contract and their respective security classification levels;
- b) a list of premises in which Classified Information is generated or managed;
- c) the procedure for the communication about the changes and about validity in the security classification levels of the transferred information;
- d) the procedure for the transportation of Classified Information;
- e) an obligation to notify any actual or suspected Breach of Security .

3. A copy of the security annex shall be forwarded to the National Security Authority of the Party under whose jurisdiction the Classified Contract is to be implemented.

4. The National Security Authorities may agree on mutual visits in order to analyse the efficiency of the measures adopted by a Contractor/sub-contractor for the protection of Classified Information involved in a Classified Contract/Sub-contract.

ARTICLE 9

TRANSFER OR TRANSMISSION OF CLASSIFIED INFORMATION

1. Classified Information shall be transferred in accordance with the national legislation of the Originating Party through diplomatic channels or as otherwise agreed in writing between the National Security Authorities in accordance with their national legislation.

2. If a large consignment containing Classified Information is to be transferred the National Security Authorities shall agree upon the means of transportation, the route and security measures for each such case.

3. The Parties may transmit Classified Information by electronic means in accordance with the security procedures approved by the National Security Authorities in writing.

4. The Recipient Party shall confirm the receipt of Classified Information in writing.

ARTICLE 10
REPRODUCTION, TRANSLATION AND DESTRUCTION
OF CLASSIFIED INFORMATION

1. Reproduction, translation and destruction of Classified information shall be made in accordance with the national legislation of the Recipient Party or otherwise agreed between the Parties in accordance with their national legislation

2. Reproduction and translation of Classified Information released under this Agreement shall bear an appropriate national security classification marking, in accordance with the equivalence stated in Article 4 and shall be protected as the originals. Number of reproductions shall be limited to that required for official purposes.

3. Translation 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.

4. Classified Information released under this Agreement marked Strict secret de importanță deosebită/„Szigorúan titkos!”/ TOP SECRET shall be translated or reproduced only upon the prior written consent of the Originating Party.

5. Classified Information released under this Agreement marked Strict secret de importanță deosebită/„Szigorúan titkos!”/ TOP SECRET shall not be destroyed. It shall be returned to the Originating Party after it is no longer considered necessary by the Recipient Party or upon request of the Originating Party.

6. 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, in such a manner as to eliminate its reconstruction in part or in whole. 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 coordination 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 Certificate 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 security classification level of Classified Information involved;
- f) name and address of the facility to be visited, as well as the name, phone/fax number, e-mail address of its point of contact;
- g) date, signature and stamping of the official seal of the 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 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, cooperate in the investigation.

3. In case the Breach of Security occurs on the territory of a third state the National Security Authority of the dispatching Party shall take all necessary measures in order to ensure that the actions prescribed in paragraph 2 are initiated.

4. 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 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 consent of the Parties in writing. Such amendments shall enter into force in accordance with Paragraph 1.

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.

6. When this Agreement enters into force, the *Agreement between the Government of Romania and the Government of the Republic of Hungary on the mutual protection of the exchanged state secret military information, signed at Debrecen, on the 17th of February, 1997* and the *Agreement for Changing Article 1 of the Agreement between the Government of Romania and the Government of the Republic of Hungary on the mutual protection of the exchanged state secret military information, signed at Arad 17th of October, 2002* shall be terminated.

Done in **BUCHAREST** on **2 October 2018** in two originals, in Romanian, Hungarian and English languages, all texts being equally authentic. In case of differences in interpretation the English text shall prevail.

In witness of which, the undersigned, duly authorised to this effect, have signed this Agreement.

FOR ROMANIA

FOR HUNGARY

Copie certificată pentru conformitate cu
originalul

Corina Badea, director

Direcția Tratatelor Internaționale