

ACORD DE SECURITATE

ÎNTRE

GUVERNUL ROMÂNIEI

ȘI

GUVERNUL REPUBLICII SLOVACE

**PRIVIND PROTECȚIA RECIPROCĂ A
INFORMAȚILOR CLASIFICATE**



Guvernul României și Guvernul Republicii Slovace, denumite în continuare Părți Contractante,

În scopul asigurării protecției Informațiilor Clasificate, schimbate direct sau prin intermediul altor instituții publice ori persoane juridice care gestionează Informații Clasificate din statul celeilalte Părți Contractante, și în cadrul activităților din sfera de competență a Autorităților Competente de Securitate din statele Părților Contractante

Au convenit următoarele:

ARTICOLUL 1 DOMENIUL DE APLICARE

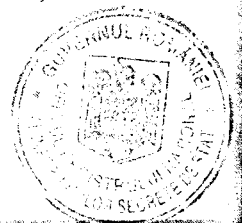
(1) Prezentul Acord de Securitate (denumit în continuare Acord) va constitui baza legală a tuturor activităților ce implică schimbul de Informații Clasificate între Părțile Contractante, prin intermediul Autorităților Competente de Securitate sau prin intermediul altor instituții publice sau persoane juridice, în conformitate cu legislațiile naționale, referitor la:

a) cooperarea între Părțile Contractante în domeniul apărării naționale și orice alte aspecte legate de securitatea națională;

b) cooperarea, activitatea societăților mixte, contractele sau alte raporturi juridice între alte instituții publice ori persoane juridice din statele Părților Contractante în domeniul apărării naționale și orice alt aspect legat de securitatea națională;

c) vânzarea de echipamente, produse și know-how.

(2) Prezentul Acord nu va afecta obligațiile Părților Contractante sau ale statelor lor ce derivă din dreptul internațional. Prezentul Acord nu va fi folosit împotriva intereselor, securității și integrității teritoriale ale altor state.



ARTICOLUL 2 DEFINIȚII

În sensul prezentului Acord:

a) **Informație Clasificată** înseamnă:
orice informație, document sau material, indiferent de forma sa fizică și căreia i s-a atribuit un anumit nivel de clasificare în conformitate cu legislațiile naționale și care va fi protejat corespunzător;

b) **Document Clasificat** înseamnă:
orice tip de înregistrare ce conține Informații Clasificate indiferent de formă sau caracteristică fizică, incluzând, dar fără a se limita la, materiale scrise sau tipărite, cartele și benzi de procesare a datelor, hărți, grafice, fotografii, picturi, desene, gravuri, schițe, note și documente de lucru, copii la indigo și riboane de tipărit sau multiplicări efectuate prin orice mijloace sau metode, înregistrări audio, vocale, magnetice, electronice, optice sau video sub orice formă, cât și echipamente portabile de procesare automată a datelor cu medii fixe de stocare și detașabile;

c) **Material Clasificat** înseamnă:
orice obiect sau parte a unui mecanism, prototip, echipament, armă etc. fabricat, mecanic sau manual ori aflat în curs de fabricație și căreia i s-a atribuit un nivel de Clasificare de Securitate;

d) **Clasificare de Securitate** înseamnă:
atribuirea unui nivel de clasificare de securitate, în conformitate cu legislațiile naționale ale statelor Părților Contractante;

e) **Contract Clasificat** înseamnă:
un acord între doi sau mai mulți Contractanți prin care se stabilesc și se definesc drepturile și obligațiile acestora și care conține sau implică Informații Clasificate;

f) **Contractant sau Subcontractant** înseamnă:
o persoană juridică ce are capacitatea legală de a încheia Contracte Clasificate;



g) Incident de Securitate înseamnă:
o acțiune sau inacțiune contrară legislațiilor naționale a cărei consecință a determinat sau este de natură să determine compromiterea Informației Clasificate;

h) Compromitere a Informației Clasificate înseamnă:
situație când - datorită unui Incident de Securitate sau unei activități ostile (precum spionaj, act de terorism sau furt) Informațiile Clasificate și-au pierdut confidențialitatea, integritatea, autenticitatea ori disponibilitatea sau când serviciile și resursele ajutoare și-au pierdut integritatea sau disponibilitatea. Aceasta include pierderea, divulgarea, parțială sau totală, modificarea ori distrugerea neautorizată sau refuzul serviciului;

i) Anexă de Securitate înseamnă:
un document emis de către autoritatea îndreptățită a statului Părții Contractante emitente ca parte a oricărui Contract sau Subcontract Clasificat, ce identifică cerințele de securitate sau acele elemente ale contractului clasificat care necesită protecție de securitate;

j) Listă a Clasificărilor de Securitate înseamnă:
evidența informațiilor, materialelor și activităților clasificate aferente unui Contract Clasificat și clasificarea de securitate a acestora, inclusă în Anexa de Securitate;

k) Certificat de Securitate a Personalului înseamnă:
document care atestă faptul că, în exercitarea atribuțiilor profesionale, posesorul acestuia poate avea acces la Informații Clasificate de un anumit nivel de secretizare, potrivit principiului Necesității de a Cunoaște;

l) Certificat de Securitate Industrială înseamnă:
document prin care se atestă că o persoană juridică este abilitată să deruleze activități industriale care presupun accesul la Informații Clasificate;

m) Necesitatea de a Cunoaște înseamnă:
principiu conform căruia accesul la Informații Clasificate se acordă în mod individual numai persoanelor care, pentru exercitarea atribuțiilor profesionale, trebuie să lucreze cu astfel de informații sau să aibă acces la acestea;



n) Autoritatea Competentă de Securitate înseamnă: instituția menționată la art. 7 învestită cu autoritate la nivel național care, conform legislației naționale, asigură implementarea unitară a măsurilor de protecție a Informațiilor Clasificate;

o) Autoritatea Desemnată de Securitate înseamnă: instituție care, conform legislației naționale, este abilitată să stabilească, pentru domeniul său de activitate și responsabilitate, structuri și măsuri proprii privind coordonarea și controlul activității referitoare la protecția Informațiilor Clasificate. Autoritatea Desemnată de Securitate este coordonată, în domeniul protecției Informațiilor Clasificate, de către Autoritatea Competentă de Securitate;

p) Terț înseamnă: orice instituție, organizație națională sau internațională, persoană juridică ce nu este parte la prezentul Acord.

ARTICOLUL 3 PROTECȚIA INFORMAȚIILOR CLASIFICATE

(1) În conformitate cu legislațiile naționale, Părțile Contractante vor lua măsuri adecvate pentru protecția Informațiilor Clasificate care sunt transmise, primite, produse sau procesate, ca rezultat al oricărui contract sau relație între persoanele juridice din statele lor. Statele Părților Contractante vor acorda tuturor Informațiilor Clasificate schimbate, primite, produse sau procesate același grad de protecție ca cel prevăzut pentru propriile Informații Clasificate cu nivel echivalent de clasificare, conform art. 4.

(2) Partea Contractantă primitoare și persoanele juridice din statul său nu vor utiliza un nivel mai scăzut de Clasificare de Securitate pentru Informațiile Clasificate primite și nici nu vor declassifica aceste informații, fără acordul prealabil scris al Autorității Competente de Securitate din statul Părții Contractante emitente. Autoritatea Competentă de Securitate a Părții Contractante emitente va informa Autoritatea Competentă de Securitate a Părții Contractante primitoare asupra oricăror modificări survenite în Clasificarea de Securitate a informațiilor schimbate.

(3) Multiplicarea sau modificarea, în orice mod, a Informațiilor Clasificate primite se va face numai cu acordul scris al Părții Contractante emitente. Toate copiile de pe Informațiile Clasificate vor fi marcate cu

aceiași nivel de clasificare ca și originalul și vor fi protejate în aceeași manieră ca și informațiile originale. Numărul de copii va fi limitat la cel necesar scopurilor oficiale.

(4) Traducerea Informațiilor Clasificate poate fi făcută numai de către persoanele care dețin Certificate de Securitate a Personalului corespunzătoare nivelului de clasificare al documentului original. Traducerea va fi marcată cu același nivel de clasificare ca și documentul original.

(5) În cazul multiplicării Informației Clasificate, va fi reprodusă și marcarea Clasificării de Securitate a informației originale.

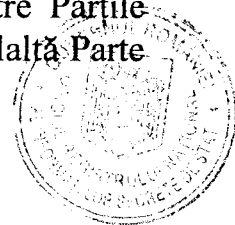
(6) Copierea Informației Clasificate marcate cu nivelul STRICT SECRET DE IMPORTANTĂ DEOSEBITĂ / PRÍSNE TAJNÉ / TOP SECRET poate fi făcută numai pe baza aprobării scrise a Autorității Competente de Securitate a statului Părții Contractante emitente.

(7) Informațiile Clasificate vor fi distruse numai cu acordul scris sau la solicitarea Părții Contractante emitente, în conformitate cu legislațiile naționale ale Părților, astfel încât reconstituirea, parțială sau integrală, a acestora să fie imposibilă. În cazul în care Partea Contractantă emitentă nu își dă acordul cu privire la distrugerea unei anumite Informații Clasificate, aceasta îi va fi returnată.

(8) Statul Părții Contractante primitoare va informa statul Părții Contractante emitente cu privire la executarea operațiunilor de distrugere. Informațiile Clasificate marcate STRICT SECRET DE IMPORTANTĂ DEOSEBITĂ / PRÍSNE TAJNÉ / TOP SECRET nu vor fi distruse și vor fi returnate Părții Contractante emitente. În caz de pericol iminent, aceste informații pot fi distruse fără autorizare prealabilă. Această situație trebuie imediat notificată Autorității Competente de Securitate a statului Părții Contractante emitente.

(9) Accesul la Informații Clasificate ori în obiectivele în care se desfășoară activități ce implică utilizarea Informațiilor Clasificate sau unde se stochează astfel de informații va fi permis numai persoanelor care posedă Certificat de Securitate a Personalului corespunzător, cu respectarea principiului Necesitatea de a Cunoaște.

(10) Prezentul Acord nu va fi invocat de nici una dintre Părțile Contractante pentru a obține Informațiile Clasificate pe care cealaltă Parte Contractantă le-a primit de la un Terț.



(11) Statul fiecărei Părți Contractante va urmări respectarea legislației naționale de către persoanele juridice care dețin, procesează, produc sau utilizează Informații Clasificate ale statului celeilalte Părți Contractante, în special prin intermediul vizitelor de analiză.

ARTICOLUL 4 CLASIFICĂRILE DE SECURITATE

(1) Clasificările de Securitate aplicabile pentru marcarea Informațiilor Clasificate schimbate în cadrul prezentului Acord vor fi:

a) pentru România: SECRET DE SERVICIU (RESTRICTED), SECRET (CONFIDENTIAL), STRICT SECRET (SECRET) și STRICT SECRET DE IMPORTANTĂ DEOSEBITĂ (TOP SECRET);

b) pentru Republica Slovacă: VYHRADENÉ (RESTRICTED), DÔVERNÉ (CONFIDENTIAL), TAJNÉ (SECRET) și PRÍSNE TAJNÉ (TOP SECRET).

(2) Părțile Contractante au stabilit echivalența Clasificărilor de Securitate după cum urmează:

România	Republica Slovacă	Echivalență în limba engleză
STRICT SECRET DE IMPORTANTĂ DEOSEBITĂ	PRÍSNE TAJNÉ	TOP SECRET
STRICT SECRET	TAJNÉ	SECRET
SECRET	DÔVERNÉ	CONFIDENTIAL
SECRET DE SERVICIU	VYHRADENÉ	RESTRICTED

ARTICOLUL 5 CERTIFICATUL DE SECURITATE

(1) Fiecare Parte Contractantă va garanta faptul că orice persoană care, în exercitarea funcției, necesită acces la Informații Clasificate deține un Certificat de Securitate a Personalului valabil emis în conformitate cu legislațiile naționale în domeniu și de nivel corespunzător.



(2) La cerere, Autoritățile Competente de Securitate din statele Părților Contractante își vor acorda asistență reciprocă în procedurile de vetting privind emiterea Certificatelor de Securitate a Personalului și a Certificatelor de Securitate Industrială, în conformitate cu legislațiile naționale ale acestora.

(3) Statele Părților Contractante vor recunoaște reciproc Certificatele de Securitate a Personalului și Certificatele de Securitate Industrială emise potrivit legislațiilor naționale.

(4) Autoritățile Competente de Securitate se vor informa reciproc asupra oricăror modificări ale Certificatelor de Securitate a Personalului și Certificatelor de Securitate Industrială care sunt relevante în privința activităților desfășurate în baza Acordului, în special asupra retragerii sau a reducerii nivelului de acces în baza acestora.

ARTICOLUL 6 DISEMINAREA INFORMAȚIILOR CLASIFICATE

(1) Diseminarea Informațiilor Clasificate către Terți poate avea loc numai în baza acordului prealabil scris al Autorității Competente de Securitate din statul Părții Contractante emitente, care poate impune noi limitări asupra diseminării.

(2) Fiecare Parte Contractantă se va asigura că Informațiile Clasificate primite de la cealaltă Parte Contractantă sunt utilizate numai în scopul pentru care au fost transmise.

ARTICOLUL 7 AUTORITĂȚILE COMPETENTE DE SECURITATE

Autoritățile Competente de Securitate responsabile, la nivel național, de implementarea și controlul măsurilor luate în aplicarea prevederilor prezentului Acord sunt:



În România	În Republica Slovacă
Guvernul României Oficiul Registrului Național al Informațiilor Secrete de Stat (ORNISS) București – Str. Mureș nr. 4, Sector 1 ROMÂNIA	Národný Bezpečnostný Úrad Budatínska 30 85007 Bratislava REPUBLICA SLOVACĀ

ARTICOLUL 8 VIZITE

(1) Autoritățile Competente de Securitate vor conveni asupra vizitelor reciproce efectuate de către cetățenii statelor lor.

(2) Vizitele în obiectivele unde se procesează, se gestionează sau se stochează Informații Clasificate ori unde se desfășoară activitățile prevăzute la art.1 vor fi autorizate pentru vizitatorii din statul celeilalte Părți Contractante numai de către Autoritatea Competentă de Securitate/ Autoritatea Desemnată de Securitate din statul respectiv.

(3) Cererea pentru vizită va fi trimisă statului gazdă de regulă cu 10 zile lucrătoare înainte de efectuarea vizitei planificate.

(4) Cererea pentru vizită va conține următoarele:

a) numele și prenumele vizitatorului, data și locul nașterii, numărul pașaportului;

b) naționalitatea;

c) funcția vizitatorului și instituția ori compania pe care o reprezintă, sau denumirea ori elementele de identificare ale Contractului Clasificat în care este implicat;

d) informații privind nivelul de acces în baza Certificatului de Securitate a Personalului al vizitatorului;

e) scopul vizitei și data estimată a sosirii și a plecării;



f) denumirea instituției sau companiei care urmează să fie vizitată.

(5) În cazul unor vizite repetate, Autoritățile Competente de Securitate/Autoritățile Desemnate de Securitate aprobă listele cu vizitele regulate. Aceste liste au o valabilitate de maximum 12 luni.

(6) Proceduri detaliate referitoare la vizite vor fi elaborate și convenite între Autoritățile Competente de Securitate/ Autoritățile Desemnate de Securitate.

(7) Fiecare Parte Contractantă va garanta protecția datelor personale ale vizitatorilor în conformitate cu legislația națională.

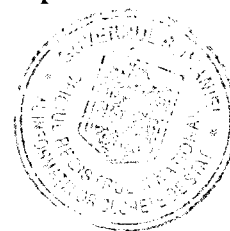
ARTICOLUL 9 SECURITATEA INDUSTRIALĂ

(1) În cazul în care una dintre Părțile Contractante sau persoanele juridice din statul acesteia intenționează să atribuie un Contract Clasificat ce urmează a se derula pe teritoriul statului celeilalte Părți Contractante, atunci Partea Contractantă din statul în care se derulează Contractul Clasificat își va asuma responsabilitatea de a proteja Informațiile Clasificate referitoare la contract, în conformitate cu legislația sa națională.

(2) Înainte de diseminarea către Contractanți/ Subcontractanți sau potențiali Contractanți/ Subcontractanți a oricăror Informații Clasificate primite de la cealaltă Parte Contractantă, Partea Contractantă primitoare, prin intermediul Autorității Competente de Securitate, va trebui să întreprindă următoarele:

a) să acorde un Certificat de Securitate Industrială de nivel corespunzător Contractanților/ Subcontractanți sau potențialilor Contractanți/ Subcontractanți, cu condiția ca aceștia să fi îndeplinit cerințele necesare eliberării Certificatului;

b) să acorde Certificate de Securitate a Personalului de nivel corespunzător tuturor persoanelor ale căror îndatoriri necesită acces la Informații Clasificate, cu condiția ca aceste persoane să îndeplinească cerințele necesare eliberării Certificatului.



(3) Părțile Contractante vor asigura ca fiecare Contract Clasificat să cuprindă o Anexă de Securitate corespunzătoare ce include o Listă a Clasificărilor de Securitate.

(4) Părțile Contractante vor asigura protecția drepturilor de autor, a drepturilor de proprietate industrială – inclusiv a licențelor – și a oricăror alte drepturi legate de Informațiile Clasificate schimbate între statele lor, în conformitate cu legislațiile naționale.

ARTICOLUL 10 TRANSMITEREA INFORMAȚIILOR CLASIFICATE

(1) Informațiile Clasificate se transmit prin curier diplomatic sau militar ori prin alte mijloace agreate de Autoritățile Competente de Securitate. Autoritatea Competentă de Securitate primitoare va confirma primirea Informațiilor Clasificate.

(2) În cazul transmiterii unui volum mare de Informații Clasificate, Autoritățile Competente de Securitate vor conveni și vor aproba reciproc modalitățile de transport, ruta și măsurile de securitate pentru fiecare caz în parte.

(3) Se pot utiliza și alte mijloace autorizate de transmitere sau schimb de Informații Clasificate, dacă sunt agreate de către Autoritățile Competente de Securitate.

ARTICOLUL 11 INCIDENTE DE SECURITATE ȘI COMPROMITEREA INFORMAȚIILOR CLASIFICATE

(1) În cazul producerii unui Incident de Securitate care duce la Compromiterea sau la posibilitatea Compromiterii Informațiilor Clasificate, Autoritatea Competentă de Securitate din statul în care s-a produs Incidentul de Securitate va informa cât mai curând posibil Autoritatea Competentă de Securitate din statul celeilalte Părți Contractante, va asigura investigarea de securitate adecvată a acestui caz și va lua măsurile necesare de limitare a consecințelor, în conformitate cu



legislația națională. Dacă este necesar, la cerere, Autoritățile Competente de Securitate vor coopera la investigare.

(2) În cazul în care Compromiterea Informațiilor Clasificate s-a produs într-un stat terț, Autoritatea Competentă de Securitate din statul Părții Contractante emitente va acționa conform alin. (1).

(3) După finalizarea investigației, Autoritatea Desemnată de Securitate a statului în care s-a produs Compromiterea sau o posibilă Compromitere a Informațiilor Clasificate va informa imediat în scris, prin intermediul Autorității Competente de Securitate a statului său, Autoritatea Desemnată de Securitate a statului celeilalte Părți Contractante asupra constatărilor și concluziilor rezultate.

ARTICOLUL 12 SOLUȚIONAREA DIFERENDELOR

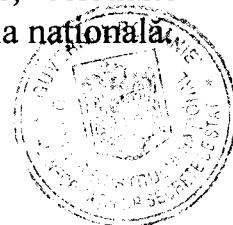
Orice diferend privind interpretarea și aplicarea prezentului Acord va fi soluționat prin consultări între Autoritățile Competente de Securitate ale statelor Părților Contractante sau, în cazul în care nu se poate ajunge la o rezolvare acceptabilă, acesta se va soluționa de către reprezentanții desemnați ai Părților Contractante.

ARTICOLUL 13 CHELTUIELI

Fiecare Parte Contractantă va suporta eventualele cheltuieli legate de implementarea prezentului Acord.

ARTICOLUL 14 ASISTENȚĂ RECIPROCĂ

(1) În scopul armonizării standardelor de securitate, fiecare Autoritate Competentă de Securitate va furniza, la cerere, celeilalte Autorități Competente de Securitate informații privind legislația națională.



(2) Fiecare Parte Contractantă va acorda asistență personalului din statul celeilalte Părți Contractante în aplicarea și interpretarea prevederilor prezentului Acord.

(3) Dacă este necesar, Autoritățile Competente de Securitate/Autoritățile Desemnate de Securitate din statele Părților Contractante se vor consulta reciproc asupra aspectelor tehnice specifice privind implementarea prezentului Acord și vor putea conveni încheierea de protocoale la prezentul Acord.

ARTICOLUL 15 DISPOZIȚII FINALE

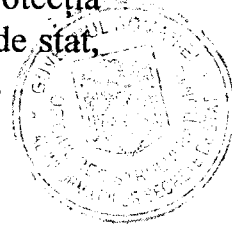
(1) Prezentul Acord este încheiat pe perioadă nedeterminată și intră în vigoare în prima zi a celei de a doua luni de la data primirii ultimei notificări scrise prin care Părțile Contractante se informează reciproc asupra îndeplinirii tuturor procedurilor interne necesare pentru intrarea în vigoare a Acordului.

(2) Fiecare Parte Contractantă poate denunța prezentul Acord oricând, în scris. În astfel de cazuri, valabilitatea Acordului va înceta după 6 (șase) luni de la data la care notificarea de denunțare a fost primită de cealaltă Parte Contractantă. Fără a ține cont de denunțarea prezentului Acord, toate Informațiile Clasificate furnizate în baza acestuia vor continua să fie protejate în conformitate cu prevederile stabilite în acest Acord.

(3) Părțile Contractante pot conveni modificarea și completarea prezentului Acord. Asemenea modificări și completări vor fi făcute în scris și vor intra în vigoare în conformitate cu prevederile alin. (1) și vor constitui parte integrantă a prezentului Acord.

(4) Fiecare Parte Contractantă va notifica prompt cealaltă Parte Contractantă asupra oricăror modificări intervenite în legislația națională, care ar putea afecta protecția Informațiilor Clasificate reglementate prin prezentul Acord.

(5) Pe data intrării în vigoare a prezentului Acord, Acordul între Guvernul României și Guvernul Republicii Slovace privind protecția reciprocă a informațiilor, a materialelor și a documentelor secrete de stat, semnat la Bratislava la 3 septembrie 1999 își va înceta valabilitatea.



Semnat la București la 6 martie 2007, în două exemplare originale, fiecare în limbile română, slovacă și engleză, toate textele fiind egal autentice. În cazul diferențelor în interpretare, textul în limba engleză va prevala.

**PENTRU
GUVERNUL ROMÂNIEI**



Prof.dr. MARIUS PETRESCU

Secretar de Stat

Directorul General

**al Oficiului Registrului Național
al Informațiilor Secrete de Stat**

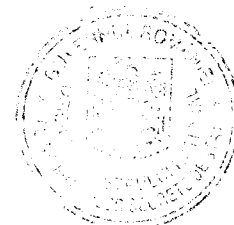
**PENTRU
GUVERNUL REPUBLICII
SLOVACE**



FRANTIŠEK BLANÁRIK

Directorul

Autorității Naționale de Securitate



BEZPEČNOSTNÁ DOHODA

MEDZI

VLÁDOU RUMUNSKA

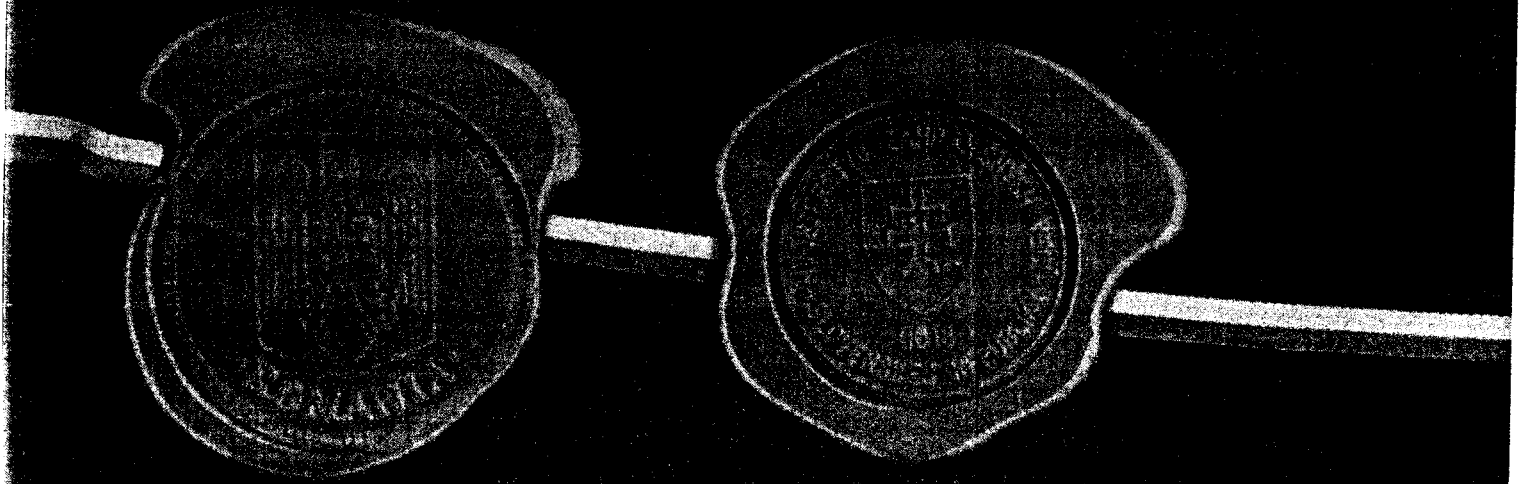
A

VLÁDOU SLOVENSKEJ REPUBLIKY

O VZÁJOMNEJ OCHRANE UTAJOVANÝCH

SKUTOČNOSTÍ





Vláda Rumunska
a
vláda Slovenskej republiky

(ďalej len „zmluvné strany“),

majúc v úmysle zabezpečiť ochranu utajovaných skutočností vymieňaných priamo alebo prostredníctvom iných štátnych orgánov alebo právnických osôb, ktoré zaobchádzajú s utajovanými skutočnosťami štátu druhej zmluvnej strany a v rámci činností, ktoré spadajú do pôsobnosti kompetentných bezpečnostných orgánov štátov zmluvných strán

dohodli sa t a k t o :

Článok 1
Použitie

(1) Táto bezpečnostná dohoda (ďalej len „dohoda“) predstavuje právny základ pre činnosti zahŕňajúce výmenu utajovaných skutočností medzi zmluvnými stranami prostredníctvom kompetentných bezpečnostných orgánov alebo prostredníctvom iných štátnych orgánov alebo právnických osôb v súlade s vnútroštátnymi právnymi predpismi v nasledujúcich prípadoch:

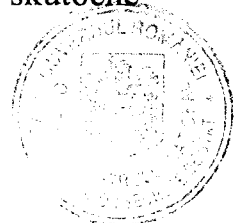
- a) spolupráca medzi zmluvnými stranami týkajúca sa obrany štátu a iných otázok vzťahujúcich sa na národnú bezpečnosť,
- b) spolupráca, spoločný podnik, zmluvný alebo akýkoľvek iný vzťah medzi štátnymi orgánmi alebo právnickými osobami štátov zmluvných strán v oblasti národnej bezpečnosti a iných otázok týkajúcich sa národnej bezpečnosti,
- c) predaj zariadenia, produktov a know-how.

(2) Touto dohodou nie sú dotknuté záväzky žiadnej zo zmluvných strán alebo ich štátov, ktoré vyplývajú z medzinárodného práva. Táto dohoda sa nepoužije proti záujmom, bezpečnosti a teritoriálnej integrite iných štátov.

Článok 2 Vymedzenie pojmov

Na účely tejto dohody :

- a) „utajované skutočnosti“ sú informácie, dokumenty alebo materiály bez ohľadu na ich fyzickú formu, ktorým bol určený konkrétny stupeň utajenia v súlade s vnútroštátnymi právnymi predpismi a ktoré sú podľa toho chránené,
- b) „utajovaný dokument“ je akýkoľvek záznam obsahujúci utajované skutočnosti, bez ohľadu na svoju formu alebo fyzickú charakteristiku, zahŕňajúc, bez obmedzenia, písané alebo tlačené materiály, pásky a karty na spracovanie údajov, mapy, tabuľky, fotografie, maľby, výkresy, rytiny, škice, pracovné poznámky a papiere, priekleповé papiere a atramentové pásky alebo reprodukcie akýmkoľvek prostriedkami alebo procesmi a hlasové, zvukové, magnetické, elektronické, optické alebo obrazové záznamy v akejkoľvek forme a prenosné zariadenie ADP s uloženým počítačovým pamäťovým médium a vyberateľným počítačovým pamäťovým médium,
- c) „utajovaný materiál“ je akýkoľvek predmet alebo časť strojového zariadenia, prototypu, vybavenia alebo zbrane, vyhotovený mechanicky alebo ručne, ktorý je už vyrobený alebo jeho výroba prebieha, a ktorému bol priradený stupeň utajenia,
- d) „stupeň utajenia“ je pridelenie stupňa utajenia v súlade s vnútroštátnymi právnymi predpismi štátov zmluvných strán,
- e) „utajovaný kontrakt“ je dohoda medzi dvoma alebo viacerými kontrahentmi, ktorá zakladá alebo definuje ich práva a povinnosti a obsahuje alebo zahŕňa utajované skutočnosti,
- f) „kontrahent alebo subkontrahent“ je právnická osoba, ktorá je právne spôsobilá uzatvárať utajované kontrakty,
- g) „porušenie bezpečnosti“ je konanie alebo opomenutie konania v rozpore s vnútroštátnymi právnymi predpismi, ktorého výsledkom je skutočné alebo možné ohrozenie utajovanej skutočnosti,



- h) „ohrozenie utajovanej skutočnosti“ je situácia, keď – v dôsledku porušenia bezpečnosti alebo nepriateľskej činnosti (ako je špionáž, teroristický čin alebo krádež) - utajovaná skutočnosť stratila dôvernosť, integritu, pravosť alebo dostupnosť, alebo podporné služby alebo zdroje stratili svoju integritu alebo dostupnosť. Toto zahŕňa stratu, čiastočné alebo úplné poskytnutie, neoprávnenú modifikáciu alebo zničenie ako aj odmietnutie služby,
- i) „list o bezpečnostných aspektoch“ je dokument vydaný príslušným orgánom štátu poskytujúcej zmluvnej strany ako časť akéhokoľvek utajovaného kontaktu alebo subkontraktu, identifikujúci bezpečnostné požiadavky alebo tie prvky kontraktu, ktoré vyžadujú bezpečnostnú ochranu,
- j) „kontrolný zoznam stupňov utajenia“ je zoznam utajovaných skutočností, materiálov alebo aktivít súvisiacich s utajovaným kontraktom a s ich stupňami utajenia, zahrnutými v liste o bezpečnostných aspektoch,
- k) „osvedčenie o previerke personálnej bezpečnosti“ je dokument potvrdzujúci, že pri výkone svojich povinností, môže mať držiteľ prístup k utajovaným skutočnostiam určitého stupňa utajenia v súlade s princípom potreby vedieť,
- l) „potvrdenie o priemyselnej bezpečnosti“ je dokument potvrdzujúci, že právnická osoba je oprávnená vykonávať priemyselné činnosti vyžadujúce prístup k utajovaným skutočnostiam,
- m) „potreba vedieť (need-to-know)“ je princíp, na základe ktorého prístup k utajovaným skutočnostiam môže byť udelený jednotlivo, len tým osobám, ktoré pre výkon svojich povinností potrebujú pracovať s alebo mať prístup k utajovaným skutočnostiam,
- n) „kompetentný bezpečnostný orgán“ je inštitúcia uvedená v článku 7, splnomocnená na národnej úrovni, ktorá v súlade s vnútroštátnymi právnymi predpismi zabezpečuje jednotnú implementáciu ochranných opatrení pre utajované skutočnosti,
- o) „určený bezpečnostný orgán“ je inštitúcia, ktorá v súlade s vnútroštátnymi právnymi predpismi je splnomocnená stanoviť, pre svoju činnosť a oblasť zodpovednosti, svoje vlastné štruktúry a opatrenia týkajúce sa koordinácie a kontroly činnosti v oblasti ochrany utajovaných skutočností. Určený bezpečnostný orgán je v oblasti

ochrany utajovaných skutočností koordinovaný kompetentným bezpečnostným orgánom,

„tretia strana“ je každá inštitúcia, národná organizácia alebo medzinárodná organizácia, alebo právnická osoba, ktoré nie je stranou tejto dohody.

Článok 3

Ochrana utajovaných skutočností

(1) V súlade s vnútroštátnymi právnymi predpismi zmluvné strany prijímú nevyhnutné opatrenia potrebné na ochranu utajovaných skutočností, ktoré sa týkajú, prenášajú, prijímajú, tvoria alebo spracúvajú ako výsledok zmluvného alebo iného vzťahu medzi právnickými osobami svojich štátov. Štáty zmluvných strán poskytnú všetkým vymieňaným, prijatým, vytvoreným alebo vyvinutým utajovaným skutočnostiam úroveň ochrany zodpovedajúcu stupňu utajenia podľa ekvivalencie uvedenej v článku 4.

(2) Prijímajúca zmluvná strana a právnické osoby jej štátu nepoužijú nižší stupeň utajenia pre prijaté utajované skutočnosti ani ich neodtajnia bez predchádzajúceho písomného súhlasu kompetentného bezpečnostného orgánu štátu poskytujúcej zmluvnej strany. Kompetentný bezpečnostný orgán štátu poskytujúcej zmluvnej strany informuje kompetentný bezpečnostný orgán štátu prijímajúcej zmluvnej strany o akýchkoľvek zmenách stupňa utajenia vymieňaných utajovaných skutočností.

(3) Rozmnožovanie alebo akúkoľvek modifikáciu prijatých utajovaných skutočností je možné vykonať len s písomným súhlasom poskytujúcej zmluvnej strany. Všetky kópie utajovaných skutočností sa označia rovnakým stupňom utajenia ako originál a chránia sa rovnako ako pôvodné utajované skutočnosti. Počet kópií je obmedzený len na počet potrebný na oficiálne účely.

(4) Preklad utajovaných skutočností môžu vykonávať len osoby, ktorým bolo vydané osvedčenie o previerke personálnej bezpečnosti zodpovedajúce stupňu utajenia pôvodného dokumentu. Preklad musí byť označený rovnakým stupňom utajenia ako pôvodný dokument.

(5) V prípade reprodukcie utajovaných skutočností musí byť reprodukovaný aj ich pôvodný stupeň utajenia.



(6) Kópie utajovaných skutočností označených STRICT SECRET DE IMPORTANTĂ DEOSEBITĂ / PRÍSNE TAJNÉ/ TOP SECRET je možné vykonať len na základe písomného súhlasu kompetentného bezpečnostného orgánu štátu poskytovajúcej zmluvnej strany.

(7) Utajované skutočnosti sa zničia len s písomným súhlasom alebo na požiadanie štátu poskytovajúcej zmluvnej strany v súlade s vnútroštátnymi právnymi predpismi tak, aby akákoľvek možnosť obnovy utajovaných skutočností ako celku alebo ich časti bola vylúčená. Ak štát poskytovajúcej zmluvnej strany nesúhlasí so zničením niektorých utajovaných skutočností, tieto sa mu vrátia.

(8) Štát prijímajúcej zmluvnej strany informuje štát poskytovajúcej zmluvnej strany o zničení utajovaných skutočností. Utajované skutočnosti označené STRICT SECRET DE IMPORTANTĂ DEOSEBITĂ / PRÍSNE TAJNÉ/ TOP SECRET sa nezničia, ale sa vrátia štátu poskytovajúcej zmluvnej strany. V prípade bezprostredného ohrozenia sa tieto utajované skutočnosti môžu zničiť aj bez predchádzajúceho súhlasu. Kompetentný bezpečnostný orgán štátu poskytovajúcej zmluvnej strany je o tom bezodkladne informovaný.

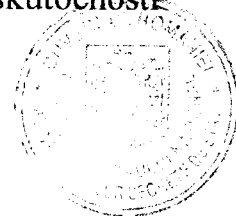
(9) Prístup k utajovaným skutočnostiam alebo na miesta, kde sa vykonávajú činnosti zahŕňajúce utajované skutočnosti alebo kde sa utajované skutočnosti uchovávajú, je obmedzený len na osoby s príslušným osvedčením o preverke personálnej bezpečnosti pri dodržaní princípu potreby vedieť.

(10) Žiadna zo zmluvných strán nepoužije túto dohodu na získanie utajovaných skutočností, ktoré druhá zmluvná strana získala od tretej strany.

(11) Každý štát zmluvnej strany dohliada na dodržiavanie vnútroštátnych právnych predpisov u právnických osôb, ktoré majú, vyvíjajú, vytvárajú alebo používajú utajované skutočnosti štátu druhej zmluvnej strany, prostredníctvom, okrem iného, kontrolných návštev.

Článok 4 Stupne utajenia

(1) Stupne utajenia použiteľné na označovanie utajovaných skutočností vymenovaných v rámci tejto dohody sú:



- a) pre Rumunsko SECRET DE SERVICIU (RESTRICTED), SECRET (CONFIDENTIAL), STRICT SECRET (SECRET) a STRICT SECRET DE IMPORTANTĂ DEOSEBITĂ (TOP SECRET);
- b) pre Slovenskú republiku VYHRADENÉ (RESTRICTED), DÔVERNÉ (CONFIDENTIAL), TAJNÉ (SECRET) a PRÍSNE TAJNÉ (TOP SECRET).

(2) Zmluvné strany stanovili ekvivalenciu stupňov utajenia nasledovne:

STRICT SECRET DE IMPORTANTĂ DEOSEBITĂ	PRÍSNE TAJNÉ	TOP SECRET
STRICT SECRET	TAJNÉ	SECRET
SECRET	DÔVERNÉ	CONFIDENTIAL
SECRET DE SERVICIU	VYHRADENÉ	RESTRICTED

Článok 5 Bezpečnostná previerka

- (1) Štát každej zmluvnej strany zabezpečí, aby osoba, ktorá pre výkon svojej funkcie alebo pracovné zaradenie potrebuje prístup k utajovaným informáciám, mala platné osvedčenie o previerke personálnej bezpečnosti korešpondujúce s príslušným stupňom utajenia, vydané v súlade s príslušnými vnútroštátnymi právnymi predpismi.
- (2) Kompetentné bezpečnostné orgány štátov zmluvných strán si na požiadanie navzájom poskytnú pomoc pri previerkovom procese, ktorý súvisí s vydaním osvedčenia o previerke personálnej bezpečnosti a potvrdenia o priemyselnej bezpečnosti, v súlade s ich vnútroštátnymi právnymi predpismi.
- (3) Štáty zmluvných strán si navzájom uznajú osvedčenia o previerke personálnej bezpečnosti a potvrdenia o priemyselnej bezpečnosti vydané v súlade s vnútroštátnymi právnymi predpismi.
- (4) Kompetentné bezpečnostné orgány sú povinné sa navzájom informovať o akýchkoľvek zmenách v osvedčeniach o previerke personálnej bezpečnosti a potvrdeniach o priemyselnej bezpečnosti, ktoré

sú spojené s činnosťami vykonávanými podľa tejto dohody, predovšetkým v prípade ich zrušenia alebo zníženia stupňa ich oprávnenia.

Článok 6 Poskytnutie utajovaných skutočností

(1) Poskytnutie utajovaných skutočností tretej strane sa môže uskutočniť len s písomným súhlasom kompetentného bezpečnostného orgánu štátu poskytujúcej zmluvnej strany, ktorá môže s poskytnutím viazať ďalšie obmedzenia.

(2) Každá zmluvná strana zabezpečí, že utajované skutočnosti prijaté od druhej zmluvnej strany sa použijú len na účel, na ktorý boli poskytnuté.

Článok 7 Kompetentné bezpečnostné orgány

Kompetentnými bezpečnostnými orgánmi zodpovednými na národnej úrovni za realizáciu a príslušnú kontrolu opatrení prijatých pri realizácii tejto dohody sú:

v Rumunsku:	v Slovenskej republike:
Guvernul României Oficiul Registrului Național al Informațiilor Secrete de Stat București, str. Mureș nr. 4, sect. 1 Romania	Národný bezpečnostný úrad Budatínska 30 850 07 Bratislava Slovenská republika

Článok 8 Návštevy

(1) Kompetentné bezpečnostné orgány sa dohodnú na vzájomných návštevách, vlastnými štátnymi príslušníkmi.

(2) Návštevy priestorov, v ktorých sa utajované skutočnosti vyvíjajú, vytvárajú, zaobchádza sa s nimi alebo sú uskladnené, alebo kde sa



vykonávajú činnosti uvedené v článku 1, povolí len kompetentný bezpečnostný orgán/určený bezpečnostný orgán príslušného štátu návštevníkom zo štátu druhej zmluvnej strany.

(3) Žiadosť o povolenie návštevy je potrebné zaslať hostiteľskému štátu spravidla v lehote desať pracovných dní pred plánovanou návštevou.

(4) Žiadosť o povolenie návštevy musí obsahovať tieto údaje:

- a) meno a priezvisko, dátum a miesto narodenia a číslo cestovného pasu návštevníka,
- b) štátnu príslušnosť návštevníka,
- c) funkciu návštevníka a názov subjektu, ktorý zastupuje, prípadne názov a ďalšiu bližšiu identifikáciu utajovaného kontraktu, na ktorom sa podieľa,
- d) informáciu o stupni osvedčenia o previerke personálnej bezpečnosti návštevníka,
- e) účel návštevy a predpokladaný dátum príchodu a odchodu,
- f) údaje týkajúce sa subjektu, ktorý má byť navštívený.

(5) V prípadoch opakovaných návštev kompetentné bezpečnostné orgány/určené bezpečnostné orgány schvália zoznamy pravidelných návštevníkov. Platnosť týchto zoznamov je najviac dvanásť mesiacov.

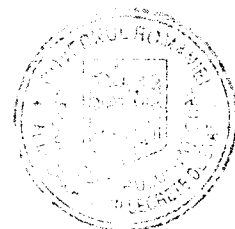
(6) Kompetentné bezpečnostné orgány/určené bezpečnostné orgány vypracujú a schvália podrobné návštevne pravidlá.

(7) Každá zmluvná strana zabezpečí ochranu osobných údajov návštevníkov v súlade s vnútroštátnymi právnymi predpismi.

Článok 9

Priemyselná bezpečnosť

(1) V prípade, že ktorákoľvek zmluvná strana alebo právnické osoby jej štátu zamýšľajú uzavrieť utajovaný kontrakt, ktorý sa bude vykonávať na území štátu druhej zmluvnej strany, prevezme štát zmluvnej strany, v ktorom sa výkon uskutoční, zodpovednosť za ochranu utajovaných skutočností týkajúcich sa kontraktu v súlade s vlastnými vnútroštátnymi právnymi predpismi.



(2) Pred poskytnutím utajovaných skutočností prijatých od štátu druhej zmluvnej strany kontrahentom/subkontrahentom alebo potencionálnym kontrahentom/ subkontrahentom zo štátu jednej zmluvnej strany, štát prijímajúcej zmluvnej strany prostredníctvom svojho kompetentného bezpečnostného orgánu:

a) udelí potvrdenie o priemyselnej bezpečnosti príslušného stupňa kontrahentom/ subkontrahentom alebo potenciálnym kontrahentom/subkontrahentom za podmienky, že splnili všetky požiadavky na jeho udelenie;

b) udelí osvedčenie o preverke personálnej bezpečnosti príslušného stupňa všetkým osobám, ktorých povinnosti si vyžadujú prístup k utajovaným skutočnostiam, ak splnili všetky požiadavky na jeho vydanie.

(3) Zmluvné strany zabezpečia, aby každý utajovaný kontrakt obsahoval príslušný list o bezpečnostných aspektoch, ktorý zahŕňa kontrolný zoznam spôsobov utajenia.

(4) Zmluvné strany zabezpečia ochranu autorských práv, práv priemyselného vlastníctva vrátane patentov a iných práv týkajúcich sa utajovaných skutočností vymieňaných medzi ich štátmi na základe vnútroštátnych právnych predpisov.

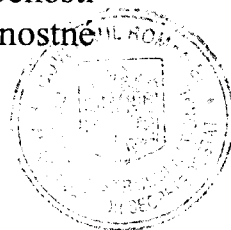
Článok 10

Preprava utajovaných skutočností

(1) Utajované skutočnosti sa prepravujú prostredníctvom diplomatických kuriérov alebo vojenských kuriérov alebo iným spôsobom, na ktorom sa dohodnú kompetentné bezpečnostné orgány. Prijímajúci kompetentný bezpečnostný orgán potvrdí prijatie utajovanej skutočnosti.

(2) Ak sa má prepraviť veľká zásielka obsahujúca utajované skutočnosti, kompetentné bezpečnostné orgány sa dohodnú a schvália spôsob prepravy, cestu a bezpečnostné opatrenia pre každý takýto prípad.

(3) Iný schválený spôsob prepravy alebo výmeny utajovaných skutočností môže byť použitý, ak sa na tom dohodnú kompetentné bezpečnostné orgány.



Článok 11

Porušenie bezpečnosti a ohrozenie utajovaných skutočností

(1) Ak došlo k porušeniu bezpečnosti, ktorého výsledkom je isté alebo predpokladané ohrozenie utajovanej skutočnosti, kompetentný bezpečnostný orgán štátu zmluvnej strany, v ktorom k porušeniu došlo, alebo čo najskôr informuje kompetentný bezpečnostný orgán štátu druhej zmluvnej strany, zabezpečí náležité vyšetrovanie tejto udalosti a prijme potrebné opatrenia na obmedzenie následkov v súlade s vnútroštátnymi bezpečnostnými predpismi. Kompetentné bezpečnostné orgány spolupracujú pri vyšetrovaní na základe žiadosti.

(2) V prípade, že ohrozenie utajovaných skutočností nastalo v tretej strane, kompetentný bezpečnostný orgán štátu odosielajúcej zmluvnej strany prijme opatrenia ako v odseku 1.

(3) Po ukončení vyšetrovania určený bezpečnostný úrad štátu, v ktorom nastalo alebo je predpokladané ohrozenie utajovaných skutočností, bezodkladne písomne informuje prostredníctvom kompetentného bezpečnostného orgánu svojho štátu určený bezpečnostný orgán štátu druhej zmluvnej strany o zisteniach a záveroch vyšetrovania.

Článok 12

Riešenie sporov

Spory týkajúce sa výkladu a realizácie tejto dohody budú predmetom konzultácií medzi kompetentnými bezpečnostnými orgánmi štátov zmluvných strán alebo, ak prijateľné riešenie nie je možné dosiahnuť, medzi určenými zástupcami zmluvných strán.

Článok 13

Náklady

Každá zmluvná strana znáša svoje vlastné náklady vo vzťahu k realizácii tejto dohody.



Článok 14 Vzájomná pomoc

- (1) Každý kompetentný bezpečnostný orgán na požiadanie poskytne druhému kompetentnému bezpečnostnému orgánu informácie o svojich vnútroštátnych právnych predpisoch, s cieľom dodržať rovnaké bezpečnostné štandardy.
- (2) Každá zmluvná strana poskytne pomoc pracovníkom štátu druhej zmluvnej strany pri výkone a výklade ustanovení tejto dohody.
- (3) V prípade potreby kompetentné bezpečnostné orgány/určené bezpečnostné orgány štátov zmluvných strán uskutočnia konzultácie k špecifickým technickým aspektom týkajúcim sa vykonávania tejto dohody a môžu dohodnúť uzavretie dodatkových protokolov k tejto dohode.

Článok 15 Záverečné ustanovenia

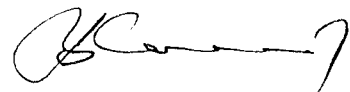
- (1) Táto dohoda sa uzatvára na neurčitý čas a nadobudne platnosť v prvý deň druhého mesiaca po prijatí neskoršieho písomného oznámenia, ktorými si zmluvné strany navzájom oznámia splnenie všetkých vnútroštátnych podmienok potrebných na nadobudnutie jej platnosti.
- (2) Každá zmluvná strana má právo kedykoľvek dohodu písomne vypovedať. V takom prípade platnosť dohody skončí šesť (6) mesiacov odo dňa doručenia oznámenia o výpovedi druhej zmluvnej strane. Napriek skončeniu platnosti tejto dohody sa bude zaobchádzať s utajovanými skutočnosťami poskytnutými na jej základe v súlade s ustanoveniami tejto dohody.
- (3) Túto dohodu možno meniť alebo dopĺňať na základe vzájomného súhlasu zmluvných strán. Zmeny a doplnky sa vykonávajú písomne a nadobudnú platnosť v súlade s ustanoveniami odseku 1 a budú tvoriť neoddeliteľnú súčasť tejto dohody.
- (4) Každá zmluvná strana bezodkladne informuje druhú zmluvnú stranu o zmenách v právnych predpisoch svojho štátu, ktoré by mali vplyv na ochranu utajovaných skutočností podľa tejto dohody.

(5) Dňom nadobudnutia platnosti nahradí táto dohoda Dohodu medzi vládou Rumunska a vládou Slovenskej republiky o vzájomnej ochrane klasifikovaných informácií, materiálov a dokumentov podpísanú v Bratislave dňa 3. septembra 1999.

Ustanovená v Bukurešti dňa 6. marca 2007, v dvoch pôvodných vyhotoveniach, ktoré sú v rumunskom, slovenskom a anglickom jazyku, pričom všetky texty majú rovnakú platnosť. V prípade rozdielnosti výkladu ustanovení tejto dohody je rozhodujúce znenie v anglickom jazyku.

Za vládu Rumunska

Za vládu Slovenskej republiky



Prof. dr. MARIUS PETRESCU

FRANTIŠEK BLANÁRIK

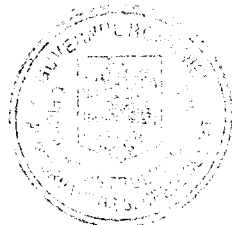
štátny tajomník

riaditeľ

generálny riaditeľ

Národného bezpečnostného úradu

Národného registračného úradu
pre utajované skutočnosti



SECURITY AGREEMENT

BETWEEN

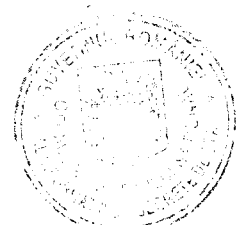
THE GOVERNMENT OF ROMANIA

AND

THE GOVERNMENT OF THE SLOVAK REPUBLIC

ON MUTUAL PROTECTION OF

CLASSIFIED INFORMATION



The Government of Romania and the Government of the Slovak Republic, hereinafter called the Contracting Parties,

in order to safeguard the Classified Information exchanged directly or through other state bodies or legal entities which deal with Classified Information of the state of the other Contracting Party and within the framework of activities which fall under the responsibility of the Competent Security Authorities of the states of the Contracting Parties,

have agreed on the following:

ARTICLE 1 APPLICABILITY

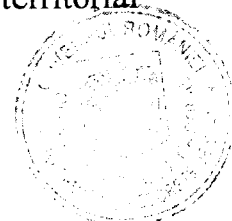
(1) This Security Agreement (hereinafter referred to as Agreement) shall form the legal basis of any activity, involving the exchange of Classified Information between the Contracting Parties through Competent Security Authorities or through other state bodies or legal entities in compliance with national legislation concerning the following

a) cooperation between the Contracting Parties concerning the state defence and any other issue related to national security;

b) cooperation, joint ventures, contractual or any other relation between state bodies or legal entities of the states of the Contracting Parties in the field of national defence and any other issue related to national security;

c) sales of equipment, products and know-how.

(2) This Agreement shall not affect the commitments of both Contracting Parties or their states which stem from international law. This Agreement shall not be used against the interests, security and territorial integrity of other states.



ARTICLE 2 DEFINITIONS

For the purpose of this Agreement:

a) **Classified Information means:**
any information, document or material, regardless of its physical form, to which a particular Security Classification has been assigned in compliance with national legislation and which shall be protected accordingly;

b) **Classified Document means:**
any sort of record containing Classified Information regardless of its form or physical characteristic, including, without limitation, written or printed matters, data processing cards and tapes, maps, charts, photographs, paintings, drawings, engravings, sketches, working notes and papers, carbon copies and ink ribbons, or reproductions produced by any means or processes, and sound, voice, magnetic, electronic, optical or video recordings in any form, as well as portable automated data processing equipment with resident computer storage media and removable computer storage media;

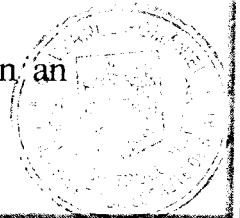
c) **Classified Material means:**
any object or item of machinery, prototype, equipment, weapon, etc., mechanically or hand made, either manufactured or in process of manufacture, to which a Security Classification has been assigned;

d) **Security Classification means:**
the assignment of degree of Security Classification in accordance with the national legislation of the states of the Contracting Parties;

e) **Classified Contract means:**
an agreement between two or more Contractors establishing or defining their rights and obligations and containing or implying Classified Information;

f) **Contractor or Subcontractor means:**
a legal entity possessing the legal capability to conclude Classified Contracts;

g) **Breach of Security means:**
an act or an omission contrary to national legislation, that results in an



actual or possible Compromise of Classified Information;

h) Compromise of Classified Information means:

a situation when – due to a Breach of Security or adverse activity (such as espionage, act of terrorism or theft) – Classified Information has lost its confidentiality, integrity, authenticity or availability or when supporting services and resources have lost their integrity or availability. This includes loss, partial or total disclosure, unauthorized modification or destruction as well as denial of service;

i) Security Aspects Letter means:

a document issued by the appropriate authority of the state of the originating Contracting Party as a part of any Classified Contract or subcontract, identifying the security requirements or the elements of the Classified Contract that require security protection;

j) Security Classification Check List means:

a listing of Classified Information, materials or activities related to a Classified Contract and their Security Classification included in the Security Aspects Letter;

k) Personnel Security Clearance Certificate means:

a document certifying that, in performing his/her duties, the holder may have access to Classified Information of a certain secrecy level in compliance with the Need to Know principle;

l) Facility Security Clearance Certificate means:

a document certifying that a legal entity is authorized to carry out industrial activities requiring access to Classified Information;

m) Need to Know means:

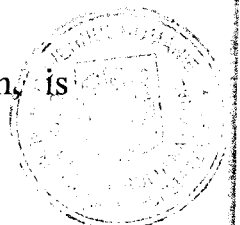
a principle by which access to Classified Information may be granted individually, only to persons who, in performing their duties, need to work with or have access to Classified Information;

n) Competent Security Authority means:

the institution listed in Article 7, empowered with authority at national level which, in compliance with the national legislation, ensures the unitary implementation of the protective measures for Classified Information;

o) Designated Security Authority means:

an institution which, in compliance with the national legislation, is



empowered to establish, for its activity and responsibility field, its own structures and measures regarding the coordination and control of the activity referring to the protection of Classified Information. The Designated Security Authority is coordinated, in the field of the protection of Classified Information, by the Competent Security Authority;

p) Third Party means:
any institution, national or international organization or legal entity which is not party to this Agreement.

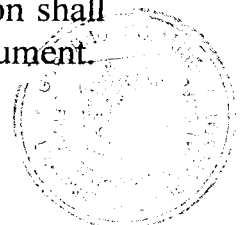
ARTICLE 3 PROTECTION OF CLASSIFIED INFORMATION

(1) In accordance with the national legislation, the Contracting Parties shall take appropriate measures to protect Classified Information which is transmitted, received, produced or developed as a result of a contractual or any other relation between the legal entities of their respective states. The states of the Contracting Parties shall afford to all of the exchanged, received, produced or developed Classified Information the level of protection corresponding to the equivalent degree of Security Classification, according to Article 4.

(2) The receiving Contracting Party and the legal entities of its state shall neither use a lower Security Classification for the received Classified Information nor declassify it without prior written consent of the Competent Security Authority of the state of the originating Contracting Party. The Competent Security Authority of the originating Contracting Party shall inform the Competent Security Authority of the receiving Contracting Party of any changes in Security Classification of the exchanged Classified Information.

(3) Reproduction or modification, by any means, of the received Classified Information shall be made only with the written consent of the originating Contracting Party. All reproductions of the Classified Information shall be marked with the same Security Classifications as the original and shall be protected in the same way. The number of copies shall be limited to that required for official purposes.

(4) Translation of Classified Information may be done only by persons holding Personnel Security Clearance Certificate corresponding to the Security Classification of the original document. The translation shall be marked with the same Security Classification as the original document.



(5) In case of reproduction of the Classified Information its original Security Classification shall be reproduced too.

(6) Copies of Classified Information marked STRICT SECRET DE IMPORTANTĂ DEOSEBITĂ/PRÍSNE TAJNÉ/TOP SECRET may be done only on the basis of prior written approval of the Competent Security Authority of the state of the originating Contracting Party.

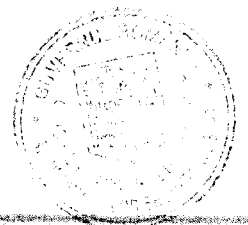
(7) Classified Information shall be destroyed in accordance with the national legislation only with prior written consent or at the request of the originating Contracting Party, in a manner preventing its reconstruction in whole or in part. Should the state of the originating Contracting Party not agree with the destruction of a particular Classified Information, this shall be returned to it.

(8) The state of the receiving Contracting Party shall inform the state of the originating Contracting Party of the destruction of Classified Information. The Classified Information marked STRICT SECRET DE IMPORTANTĂ DEOSEBITĂ/ PRÍSNE TAJNÉ/TOP SECRET shall not be destroyed but returned to the originating Contracting Party. In case of immediate danger, it may be destroyed without prior consent. The Competent Security Authority of the state of the originating Contracting Party shall immediately be notified of it.

(9) Access to Classified Information or to locations where activities involving Classified Information are performed or where Classified Information is stored, shall be allowed only to individuals having an appropriate Personnel Security Clearance Certificate, with the observance of the Need to Know principle.

(10) This Agreement shall not be invoked by either Contracting Party to obtain Classified Information that the other Contracting Party has received from any Third Party.

(11) Each state of Contracting Party shall supervise the observance of national legislation within the legal entities that hold, develop, produce or use Classified Information of the state of the other Contracting Party, by means of inter alia review visits.



ARTICLE 4 SECURITY CLASSIFICATIONS

(1) The Security Classifications applicable for marking the Classified Information exchanged within the framework of this Agreement shall be:

a) for Romania: SECRET DE SERVICIU (RESTRICTED), SECRET (CONFIDENTIAL), STRICT SECRET (SECRET) and STRICT SECRET DE IMPORTANTĂ DEOSEBITĂ (TOP SECRET);

b) for the Slovak Republic: VYHRADENÉ (RESTRICTED), DÔVERNÉ (CONFIDENTIAL), TAJNÉ (SECRET) and PRÍSNE TAJNÉ (TOP SECRET).

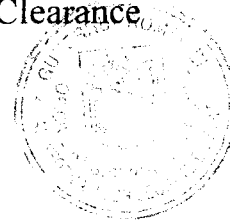
(2) The Contracting Parties have determined the equivalence of the Security Classifications as follows:

For Romania	For Slovak Republic	English Equivalent
STRICT SECRET DE IMPORTANTĂ DEOSEBITĂ	PRÍSNE TAJNÉ	TOP SECRET
STRICT SECRET	TAJNÉ	SECRET
SECRET	DÔVERNÉ	CONFIDENTIAL
SECRET DE SERVICIU	VYHRADENÉ	RESTRICTED

ARTICLE 5 SECURITY CLEARANCE

(1) Each Contracting Party shall guarantee that any individual, who, due to his/her position, needs access to Classified Information, shall hold a valid Personnel Security Clearance Certificate issued in accordance with the respective national legislation and corresponding to the appropriate Security Classification.

(2) On request, the Competent Security Authorities of the states of the Contracting Parties shall assist each other in vetting procedures related to the issue of the Personnel and Facility Security Clearance Certificates, in accordance with their national legislations.



(3) The states of the Contracting Parties shall mutually recognize Personnel and Facility Security Clearance Certificates issued in accordance with their national legislations.

(4) The Competent Security Authorities are obliged to inform each other about any changes in the Personnel and Facility Security Clearance Certificates which are connected with the activities performed according to this Agreement, especially if they have been revoked or the degree of their Security Classification has been decreased.

ARTICLE 6 RELEASE OF CLASSIFIED INFORMATION

(1) Release of Classified Information to Third Parties may take place only with prior written consent of the Competent Security Authority of the state of the originating Contracting Party, which may impose further limitations to the release.

(2) Each Contracting Party shall ensure that Classified Information received from the other Contracting Party is used for the purpose for which it has been released.

ARTICLE 7 COMPETENT SECURITY AUTHORITIES

The Competent Security Authorities responsible, at national level, for the implementation and the control of the measures undertaken in the implementation of this Agreement are:

In Romania	In the Slovak Republic
Guvernul României Oficiul Registrului Național al Informațiilor Secrete de Stat București – Str. Mureș nr.4 sect.1 ROMANIA	Národný bezpečnostný úrad Budatínska 30 85007 Bratislava SLOVAK REPUBLIC



ARTICLE 8 VISITS

(1) The Competent Security Authorities shall agree on mutual visits by their nationals.

(2) Visits to premises where Classified Information is developed, produced, handled or stored or where the activities stated in Article 1 are carried out shall be allowed only by the Competent Security Authority/Designated Security Authority of the respective state to visitors from the state of the other Contracting Party.

(3) The request for visit shall be sent to the host state, as a rule ten working days before the planned visit.

(4) The request for visit shall include:

a) name and surname of the visitor, date and place of birth, passport number;

b) visitor's nationality;

c) position of visitor and name of institution or company (s)he is representative of, or name and closer identification of Classified Contract (s)he takes part in;

d) information on the degree of Personnel Security Clearance Certificate of the visitor;

e) purpose of the visit and estimated date of arrival and departure;

f) name of institution or company to be visited.

(5) In case of repeated visits the Competent Security Authorities/Designated Security Authorities shall approve the lists of regular visitors. These lists shall be valid for twelve months at maximum.

(6) Further procedures related to visits shall be developed and agreed upon by the Competent Security Authorities/Designated Security Authorities.

(7) Each Contracting Party shall guarantee the protection of personal data of the visitors according to national legislation.

ARTICLE 9 INDUSTRIAL SECURITY

(1) In the event that either Contracting Party or legal entities of its state intend to award a Classified Contract to be performed within the territory of the state of the other Contracting Party, the Contracting Party of the state in which its performance is to take place will assume responsibility for the protection of Classified Information related to the Classified Contract in accordance with its national legislation.

(2) Prior to releasing any Classified Information received from the state of the other Contracting Party to Contractors/Subcontractors or to prospective Contractors/Subcontractors, the receiving Contracting Party shall through the Competent Security Authority of its state:

a) grant Facility Security Clearance Certificates of appropriate degree to the Contractors/Subcontractors or prospective Contractors/Subcontractors if they have met the requirements for the issue;

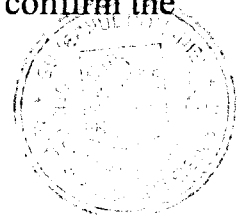
b) grant Personnel Security Clearance Certificates of appropriate degree to all personnel whose duties require access to Classified Information if they have met the requirements for the issue.

(3) The Contracting Parties shall ensure that every Classified Contract includes an appropriate Security Aspects Letter which contains a Security Classification Check-List.

(4) The Contracting Parties shall ensure protection of copyrights, industrial property rights – including patents – and any other rights connected with the Classified Information exchanged between their states, according to their national legislations.

ARTICLE 10 TRANSMISSION OF CLASSIFIED INFORMATION

(1) Classified Information shall be transmitted by diplomatic or military courier or other means agreed upon by the Competent Security Authorities. The receiving Competent Security Authority shall confirm the receipt of Classified Information.



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

(3) Other approved means of transmission or exchange of Classified Information may be used if agreed upon by the Competent Security Authorities.

ARTICLE 11 BREACH OF SECURITY AND COMPROMISE OF CLASSIFIED INFORMATION

(1) In case of a Breach of Security that results in an actual or possible Compromise of Classified Information, the Competent Security Authority of the state of the Contracting Party where it occurred shall inform as soon as possible the Competent Security Authority of the state of the other Contracting Party, shall ensure proper investigation of the event and take the necessary measures to limit the consequences, in accordance with the national legislation. If necessary, the Competent Security Authorities shall cooperate in the investigation upon request.

(2) In case the Compromise of Classified Information occurs in a third state the Competent Security Authority of the state of the dispatching Contracting Party shall take the actions stated in Paragraph 1.

(3) After completion of investigation the Designated Security Authority of the state in which the actual or possible Compromise of Classified Information occurred shall immediately inform through the Competent Security Authority of its state the Designated Security Authority of the state of the other Contracting Party on the findings and conclusions of the investigation in writing.

ARTICLE 12 SETTLEMENT OF DISPUTES

Any dispute regarding the interpretation and implementation of this Agreement shall be settled by consultation between the Competent Security Authorities of the states of the Contracting Parties or, should an acceptable settlement be impossible to reach, between the designated representatives of the Contracting Parties.



**ARTICLE 13
EXPENSES**

Each Contracting Party shall cover its own expenses related to the implementation of this Agreement.

**ARTICLE 14
MUTUAL ASSISTANCE**

(1) Each Competent Security Authority shall provide, upon request, to the other Competent Security Authority information about the national legislation, in order to keep the same security standards.

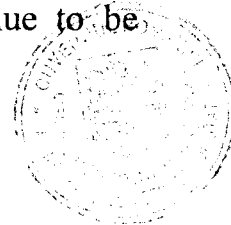
(2) Each Contracting Party shall assist personnel from the state of the other Contracting Party in the implementation and interpretation of the provisions of this Agreement.

(3) Should the need arise the Competent Security Authorities/Designated Security Authorities of the states of the Contracting Parties shall consult each other on specific technical aspects concerning the implementation of this Agreement and may agree upon conclusion of supplementary protocols to this Agreement.

**ARTICLE 15
FINAL PROVISIONS**

(1) This Agreement is concluded for an indefinite period of time and enters into force on the first day of the second month after receiving the last written notification whereby the Contracting Parties inform each other of the fulfillment of all internal procedures necessary for its entry into force.

(2) Each Contracting Party has the right to terminate this Agreement in writing at any time. In such case the validity of this Agreement shall expire after 6 (six) months following the day on which the notification of termination notice has been served to the other Contracting Party. Notwithstanding the termination of this Agreement, all Classified Information provided pursuant to this Agreement shall continue to be protected in accordance with the provisions set forth herein.



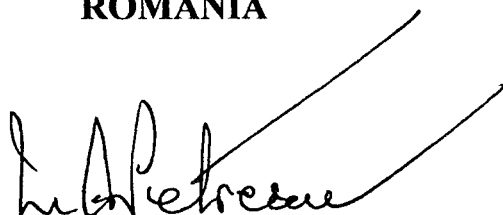
(3) This Agreement may be changed and amended on the basis of the mutual consent of the Contracting Parties. Such changes and amendments shall be made in writing, entering into force in accordance with the provisions of Paragraph 1 and shall form an inseparable part of this Agreement.

(4) Each Contracting Party shall promptly notify the other Contracting Party of any changes of its national legislation that would affect the protection of Classified Information under this Agreement.

(5) With the entry into force this Agreement shall supersede the Agreement between the Government of Romania and the Government of the Slovak Republic on mutual protection of state secret information, materials and documents, signed in Bratislava on 3rd of September 1999.

Done in Bucharest on 6th of March 2007 in two original copies, each in the Romanian, Slovak and English languages, all texts having equal validity. In case of differences of interpretation, the English text shall prevail.

**FOR THE GOVERNMENT OF
ROMANIA**



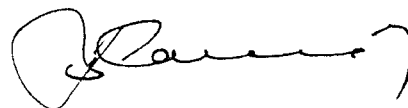
Prof. dr. MARIUS PETRESCU

Secretary of State

Director General

**of the National Registry Office
for Classified Information**

**FOR THE GOVERNMENT OF
THE SLOVAK REPUBLIC**



FRANTIŠEK BLANÁRIK

Director

of the National Security Authority

