

ACORD

ÎNTRE

GUVERNUL ROMÂNIEI

ȘI

GUVERNUL REPUBLICII SLOVENIA

PRIVIND

PROTECȚIA RECIPROCĂ A

INFORMAȚILOR CLASIFICATE

Guvernul României
și
Guvernul Republicii Slovenia,
denumite în continuare „Părți”,

în scopul asigurării protecției Informațiilor Clasificate schimbate între Părți sau între instituții de drept public și privat supuse legislației naționale proprii, luând în considerare interesele naționale și de securitate,

au convenit următoarele:

ARTICOLUL 1 DOMENIUL DE APLICARE

1. Presentul Acord va sta la baza oricărei activități care implică, în conformitate cu legislația națională a Părților, schimbul de Informații Clasificate între Părți sau între alte instituții de drept public și privat din statele acestora.
2. Presentul Acord nu va afecta obligațiile celor două Părți ce derivă din alte acorduri internaționale și nu va fi folosit împotriva intereselor, securității și integrității teritoriale ale altor state.
3. În conformitate cu legislația lor națională, Părțile vor lua toate măsurile corespunzătoare pentru a asigura protecția Informațiilor Clasificate schimbate între acestea sau generate în baza prezentului Acord.

ARTICOLUL 2 DEFINIȚII

În scopul prezentului Acord, următorii termeni sunt definiți după cum urmează:

- a) **Informații Clasificate** înseamnă orice informație, indiferent de forma sa fizică, căreia i s-a atribuit un nivel de clasificare în conformitate cu legislația națională și care va fi protejată corespunzător;
- b) **Contract Clasificat** înseamnă un contract, un sub-contract sau un proiect, inclusiv activitățile pre-contractuale, care conține Informații Clasificate sau implică accesul la acestea;

c) **Partea Emitentă** înseamnă Partea, inclusiv orice entitate de drept public sau privat, care se supune legislației naționale și care generează și transmite Informații Clasificate Părții Primitoare;

d) **Parte Primitoare** înseamnă Partea, inclusiv orice entitate de drept public sau privat, care se supune legislației naționale și care primește Informații Clasificate de la Partea Emitentă;

e) **Parte Terță** înseamnă un stat sau oricare altă entitate de drept public sau privat sau o organizație internațională care nu este parte la prezentul Acord;

f) **Necesitatea de a Cunoaște** înseamnă principiul conform căruia accesul la Informații Clasificate se poate acorda unei persoane numai în baza atribuțiilor și sarcinilor sale oficiale;

g) **Certificatul de Securitate a Personalului** înseamnă documentul emis în conformitate cu legislația națională și care certifică faptul că deținătorul poate avea acces la Informații Clasificate de un anumit nivel de clasificare;

h) **Certificatul de Securitate Industrială** înseamnă documentul emis în conformitate cu legislația națională și care certifică faptul că o persoană juridică îndeplinește condițiile necesare pentru gestionarea Informațiilor Clasificate de un anumit nivel de clasificare și este autorizată să desfășoare activități legate de un Contract Clasificat;

i) **Compromiterea Informațiilor Clasificate** înseamnă situația în care, datorită unui incident de securitate, Informațiile Clasificate și-au pierdut confidențialitatea, integritatea sau disponibilitatea.

ARTICOLUL 3

AUTORITĂȚILE COMPETENTE DE SECURITATE

1. Autoritățile Naționale de Securitate desemnate de Părți pentru a fi responsabile de implementarea generală și de controalele relevante ale tuturor aspectelor prezentului Acord sunt:

În România:

Oficiul Registrului Național al Informațiilor Secrete de Stat

În Republica Slovenia:

Urad Vlade Republike Slovenije za varovanje tajnih podatkov

2. Autoritățile Naționale de Securitate se vor informa reciproc cu privire la oricare alte autorități competente de securitate responsabile pentru implementarea prezentului Acord.
3. Părțile se vor informa reciproc cu privire la orice modificări ulterioare privind Autoritățile Naționale de Securitate.

ARTICOLUL 4

CLASIFICĂRILE DE SECURITATE

1. Informațiile Clasificate transmise în baza prezentului Acord vor fi marcate cu nivelul corespunzător al clasificării conform legislației naționale a fiecăreia dintre Părți.
2. Echivalența marcajelor naționale de clasificare de securitate este următoarea:

În România	În Republica Slovenia
STRICT SECRET DE IMPORTANTĂ DEOSEBITĂ	STROGO TAJNO
STRICT SECRET	TAJNO
SECRET	ZAUPNO
SECRET DE SERVICIU	INTERNO

ARTICOLUL 5

ACCESUL LA INFORMAȚII CLASIFICATE

1. Accesul la Informații Clasificate SECRET DE SERVICIU/INTERNO este permis numai persoanelor cărora le-a fost acordat acest acces, în conformitate cu legislația națională, care respectă principiul Necesității de a Cunoaște și au fost instruite corespunzător.
2. Accesul la Informații Clasificate SECRET/ZAUPNO și de nivel superior este permis, cu respectarea principiului Necesității de a Cunoaște, numai persoanelor cărora, în conformitate cu legislația națională, li s-a emis Certificat de Securitate a Personalului valabil pentru nivelul de clasificare al informațiilor ce urmează a fi accesate și care au fost instruite în acest sens.

3. Părțile își vor recunoaște reciproc Certificatele de Securitate a Personalului pentru acces la Informații Clasificate SECRET/ZAUPNO și de nivel superior sau autorizațiile scrise pentru acces la Informații Clasificate SECRET DE SERVICIU/INTERNO, care permit accesul la Informații Clasificate conform echivalenței din alineatul 2 al Articolului 4.

ARTICOLUL 6

PROTECȚIA INFORMAȚIILOR CLASIFICATE

1. Părțile vor asigura același nivel de protecție pentru Informațiile Clasificate care fac obiectul prezentului Acord ca și în cazul propriilor informații cu nivel de clasificare corespunzător.
2. Partea Emitentă va informa Partea Primitoare asupra oricăror condiții de transmitere sau limitări în utilizarea Informațiilor Clasificate, cât și despre orice modificări ulterioare ale clasificării.
3. Partea Primitoare se va asigura că Informațiile Clasificate sunt marcate cu nivelul de clasificare echivalent, în conformitate cu alineatul 2 al Articolului 4, precum și că nivelul de clasificare nu este schimbat, scăzut sau declassificat fără aprobarea scrisă a Părții Emitente.

ARTICOLUL 7

RESTRICȚII DE UTILIZARE A INFORMAȚIILOR CLASIFICATE

1. Partea Primitoare va utiliza Informațiile Clasificate numai în scopul pentru care acestea au fost transmise și cu respectarea restricțiilor stabilite de Partea Emitentă.
2. Partea Primitoare nu va transmite Informații Clasificate unei Părți Terțe fără acordul prealabil scris al Părții Emitente.

ARTICOLUL 8

TRANSMITEREA INFORMAȚIILOR CLASIFICATE

Informațiile Clasificate vor fi transmise între Părți prin canale diplomatice sau militare ori prin alte canale convenite de Autoritățile Naționale de Securitate, în conformitate cu legislația națională.

ARTICOLUL 9

MULTIPLICAREA, TRADUCEREA ȘI DISTRUGEREA INFORMAȚIILOR CLASIFICATE

1. Toate multiplicările și traduceri vor purta aceleași marcaje de clasificare ca și Informațiile Clasificate originale și vor fi protejate corespunzător. Traducerile și numărul de copii se vor limita la numărul minim necesar pentru scopurile oficiale.
2. Toate traduceri vor conține o adnotare corespunzătoare în limba în care au fost traduse prin care se va indica faptul că acestea conțin Informații Clasificate ale Părții Emitente, inclusiv marcajul de clasificare și numărul de referință al documentului original.
3. Informațiile Clasificate marcate STRICT SECRET DE IMPORTANTĂ DEOSEBITĂ/STROGO TAJNO vor fi multiplicare numai cu acordul scris al Părții Emitente.
4. Informațiile Clasificate marcate STRICT SECRET DE IMPORTANTĂ DEOSEBITĂ/STROGO TAJNO nu vor fi distruse. Acestea vor fi returnate Părții Emitente după ce Partea Primitoare consideră că nu îi mai sunt necesare.
5. În cazul unui pericol iminent, Informațiile Clasificate vor fi distruse fără acord prealabil. Autoritatea Națională de Securitate a Părții Emitente va fi notificată imediat despre această distrugere.
6. Informațiile Clasificate STRICT SECRET/TAJNO sau de nivel inferior vor fi distruse de către Partea Primitoare, după ce aceasta constată că nu îi mai sunt necesare, în conformitate cu legislația națională și cu acordul prealabil scris al Părții Emitente.

ARTICOLUL 10

CONTRACTE CLASIFICATE

1. Înainte de diseminarea către contractanți sau sub-contractanți a oricăror Informații Clasificate legate de un Contract Clasificat, Autoritatea Națională de Securitate a Părții Primitoare va trebui:
 - a) să confirme deținerea de către contractanții și sub-contractanții care participă la Contracte Clasificate a Certificatelor de Securitate Industrială corespunzătoare precum și deținerea, de către angajații

acestora, implicați în Contracte Clasificate, a Certificatelor de Securitate a Personalului corespunzătoare; sau

- b) să inițieze, la cerere, procedurile necesare, în conformitate cu legislația națională, pentru emiterea Certificatelor de Securitate Industrială sau a Certificatelor de Securitate a Personalului corespunzătoare.
2. Oricare dintre Autoritățile Naționale de Securitate poate solicita efectuarea inspecției de securitate a unui obiectiv pentru a asigura conformitatea permanentă cu standardele de securitate în concordanță cu legislația națională.
 3. Contractul Clasificat va conține o anexă cu prevederi referitoare la cerințele de securitate și nivelul de clasificare al fiecărui aspect sau element din Contractul Clasificat. O copie a acestei anexe va fi înaintată Autorităților Naționale de Securitate ale Părților.
 4. Părțile își vor recunoaște reciproc Certificatele de Securitate Industrială.

ARTICOLUL 11

VIZITE

1. Vizitele care necesită acces la Informații Clasificate vor fi supuse unei aprobări prealabile din partea Autorității Naționale de Securitate a Părții gazdă.
2. Solicitarea de vizită va fi transmisă Autorității Naționale de Securitate cu cel puțin 20 de zile înainte de începerea vizitei și va cuprinde următoarele date personale:
 - a) Numele și prenumele vizitatorului, data și locul nașterii, cetățenia și numărul pașaportului/documentului de identitate;
 - b) Funcția vizitatorului și specificarea angajatorului pe care acesta îl reprezintă;
 - c) Specificarea activităților la care vizitatorul va participa;
 - d) Valabilitatea și nivelul Certificatului de Securitate a Personalului deținut de vizitator, dacă este cazul;

- e) Denumirea, adresa, numărul de telefon/fax, adresa de e-mail și punctul de contact al obiectivului ce urmează a fi vizitat;
- f) Scopul vizitei, inclusiv cel mai înalt nivel al Informațiilor Clasificate ce urmează a fi accesate;
- g) Data și durata vizitei - în cazul unor vizite periodice se va specifica perioada totală acoperită de vizite;
- h) Data, semnătura și ștampila Autorității Naționale de Securitate a Părții trimițătoare.

3. În cazuri urgente, Autoritățile Naționale de Securitate pot conveni asupra unei perioade mai scurte de transmitere a solicitării de vizită.
4. Autoritățile Naționale de Securitate pot aproba de comun acord o listă cu vizitatorii îndreptățiți la vizitele periodice. Această listă va fi valabilă pe o perioadă inițială ce nu va depăși 12 luni și va putea fi extinsă pe o perioadă ulterioară ce nu va depăși 12 luni. O cerere pentru vizite periodice va fi supusă aprobării în conformitate cu paragraful 2. O dată ce lista a fost aprobată, vizitele pot fi organizate direct între instituțiile implicate.
5. Orice Informație Clasificată obținută de către un vizitator va fi considerată Informație Clasificată și va fi protejată conform prevederilor prezentului Acord.
6. Fiecare Parte va garanta protecția datelor personale ale vizitatorilor conform legislației naționale proprii.

ARTICOLUL 12

COOPERAREA DE SECURITATE

1. În scopul îndeplinirii și menținerii unor standarde comparabile de securitate, Autoritățile Naționale de Securitate își vor furniza, reciproc, la cerere, informații referitoare la standardele naționale de securitate, procedurile și practicile privind protecția Informațiilor Clasificate. În acest scop, Autoritățile Naționale de Securitate se pot vizita reciproc.
2. Autoritățile Naționale de Securitate se vor informa reciproc cu privire la riscurile de securitate care pot prejudicia Informațiile Clasificate schimbate.

3. La cerere, Autoritățile Naționale de Securitate, în conformitate cu atribuțiile proprii, se vor asista reciproc cu privire la desfășurarea procedurilor referitoare la verificările de securitate.
4. Autoritățile Naționale de Securitate se vor informa prompt asupra oricăror modificări intervenite în Certificatele de Securitate a Personalului și în Certificatele de Securitate Industrială recunoscute reciproc.
5. Serviciile de informații și de securitate ale Părților pot schimba direct informații operative și de securitate în conformitate cu legislația națională.

ARTICOLUL 13

COMPROMITEREA INFORMAȚIILOR CLASIFICATE

1. Fiecare Parte va notifica imediat, în scris cealaltă Parte cu privire la orice suspiciune sau descoperire a compromiterii Informațiilor Clasificate schimbate în baza prezentului Acord.
2. Partea Primitoare va întreprinde toate măsurile necesare posibile în conformitate cu legislația națională proprie, pentru a limita consecințele compromiterii și pentru a preveni incidentele ulterioare. La cerere, Partea Emitentă va oferi asistență în investigații; va fi informată în scris despre rezultatul investigației și despre măsurile întreprinse.

ARTICOLUL 14

CHELTUIELI

Fiecare parte va suporta propriile cheltuieli în legătură cu implementarea prezentului Acord.

ARTICOLUL 15

INTERPRETAREA ȘI SOLUȚIONAREA DIFERENDELOR

Orice diferend între Părți privind interpretarea sau aplicarea prezentului Acord va fi soluționat exclusiv prin mijloace de consultare între Părți.


ARTICOLUL 16
DISPOZIȚII FINALE

1. Presentul Acord se încheie pe o durată nedeterminată de timp. Acesta va fi supus aprobării în conformitate cu legislația națională a Părților și va intra în vigoare în prima zi din cea de-a doua lună de la data primirii ultimei notificări între Părți privind îndeplinirea procedurilor legale interne pentru intrarea în vigoare a prezentului Acord.
2. Presentul Acord poate fi modificat oricând prin acordul scris al Părților. Aceste amendamente vor intra în vigoare în conformitate cu prevederile paragrafului 1.
3. Fiecare Parte are dreptul de a denunța, oricând, în scris, prezentul Acord. În acest caz, valabilitatea Acordului va expira după 6 luni de la data la care cealaltă Parte a primit notificarea de denunțare scrisă.
4. Fără a ține cont de denunțarea prezentului Acord, toate Informațiile Clasificate transmise în baza acestuia vor continua să fie protejate în conformitate cu prevederile stabilite în prezentul Acord până când Partea Emitentă eliberează Partea Primitoare de această obligație.
5. Pentru aplicarea prezentului Acord pot fi încheiate aranjamente de implementare.

Drept dovadă subsemnații, pe deplin autorizați de guvernele lor proprii, am semnat prezentul Acord.

Semnat la București, la 29 iunie 2011, în două exemplare originale, fiecare în limbile română, slovenă și engleză, toate textele fiind egal autentice. În caz de diferențe în interpretare, textul în limba engleză va prevala.

PENTRU
GUVERNUL ROMÂNIEI



PENTRU
GUVERNUL REPUBLICII
SLOVENIA



copiază cu originalul
U. Dežman

SPORAZUM

MED

VLADO ROMUNIJE

IN

VLADO REPUBLIKE SLOVENIJE

O MEDSEBOJNEM VAROVANJU

TAJNIH PODATKOV

Vlada Romunije
in
Vlada Republike Slovenije,
v nadaljevanju pogodbenici,

sta se ob upoštevanju državnih interesov in varnosti v želji zagotoviti varovanje
tajnih podatkov, izmenjanih med njima ali med javnimi in zasebnimi subjekti v
pristojnosti njunih notranjih zakonodaj,

dogovorili:

1. ČLEN

UPORABA

1. Ta sporazum je podlaga za kakršno koli dejavnost, ki v skladu z notranjo zakonodajo pogodbenic vključuje izmenjavo tajnih podatkov med pogodbenicama ali drugimi državnimi organi ali javnimi in zasebnimi subjekti njunih držav.
2. Ta sporazum ne vpliva na obveznosti pogodbenic, ki izvirajo iz drugih mednarodnih sporazumov, in se ne uporablja v nasprotju z interesi, varnostjo in ozemeljsko celovitostjo drugih držav.
3. Pogodbenici sprejmeta v skladu s svojo notranjo zakonodajo ustrezne ukrepe za zagotovitev varovanja tajnih podatkov, ki si jih izmenjata ali nastanejo na podlagi tega sporazuma.

2. ČLEN

POMEN IZRAZOV

V tem sporazumu izrazi pomenijo:

- a) **tajni podatek** vsak podatek, ki je v skladu z notranjo zakonodajo ne glede na svojo fizično obliko označen s stopnjo tajnosti in se kot tak ustrezno varuje;
- b) **pogodba s tajnimi podatki** pogodbo, podpogodbo ali projekt, vključno s pogajanjem pred sklenitvijo pogodbe, ki vsebuje tajne podatke ali vključuje dostop do njih;

- c) **pogodbenica izvora** pogodbenico, vključno z javnimi ali zasebnimi subjekti v pristojnosti njene notranje zakonodaje, v kateri tajni podatki nastanejo in ki tajne podatke da pogodbenici prejemnici;
- d) **pogodbenica prejemnica** pogodbenico, vključno z javnimi ali zasebnimi subjekti v pristojnosti njene notranje zakonodaje, ki prejme tajne podatke od pogodbenice izvora;
- e) **tretja stran** državo ali javni ali zasebni subjekt ali mednarodno organizacijo, ki ni pogodbenica tega sporazuma;
- f) **potreba po seznanitvi** načelo, s katerim se posamezniku lahko dovoli dostop do tajnih podatkov le za opravljanje njegovih uradnih dolžnosti ali nalog;
- g) **dovoljenje za dostop do tajnih podatkov** dokument, izdan v skladu z notranjo zakonodajo, ki potrjuje, da ima imetnik lahko dostop do tajnih podatkov določene stopnje tajnosti;
- h) **varnostno dovoljenje organizacije** dokument, izdan v skladu z notranjo zakonodajo, ki potrjuje, da pravni subjekt izpolnjuje pogoje za ravnanje s tajnimi podatki določene stopnje tajnosti in je pooblaščen za izvajanje dejavnosti v zvezi s pogodbo s tajnimi podatki;
- i) **ogrožanje tajnih podatkov** razmere, v katerih tajni podatki zaradi kršitve varovanja niso več zaupni, celoviti ali razpoložljivi.

3. ČLEN

PRISTOJNI VARNOSTNI ORGANI

1. Nacionalna varnostna organa, ki sta ju pogodbenici imenovali za odgovorna za splošno izvajanje tega sporazuma in ustrezen nadzor nad vsemi njegovimi vidiki, sta:

v Romuniji:

Oficiul Registrului Național al Informațiilor Secrete de Stat.

v Republiki Sloveniji:

Urad Vlade Republike Slovenije za varovanje tajnih podatkov.

2. Nacionalna varnostna organa se uradno obveščata o drugih pristojnih varnostnih organih, odgovornih za izvajanje tega sporazuma.
3. Pogodbenici se obveščata o vseh poznejših spremembah nacionalnih varnostnih organov.

4. ČLEN

OZNAKE STOPNJE TAJNOSTI

1. Tajni podatki, dani na podlagi tega sporazuma, so označeni z ustreznimi oznakami stopnje tajnosti v skladu z notranjo zakonodajo pogodbenice.
2. Enakovredne notranje oznake stopnje tajnosti so:

Romunija	Republika Slovenija
STRICT SECRET DE IMPORTANTĂ DEOSEBITĂ	STROGO TAJNO
STRICT SECRET	TAJNO
SECRET	ZAUPNO
SECRET DE SERVICIU	INTERNO

5. ČLEN

DOSTOP DO TAJNIH PODATKOV

1. Dostop do podatkov stopnje SECRET DE SERVICIU/INTERNO je omejen na osebe, ki jim je bil tak dostop dovoljen v skladu z notranjo zakonodajo, imajo potrebo po seznanitvi in so ustrezno poučene.
2. Dostop do podatkov stopnje SECRET/ZAUPNO in višje stopnje je omejen na osebe, ki imajo potrebo po seznanitvi in jim je bilo v skladu z notranjo zakonodajo izdano dovoljenje za dostop do tajnih podatkov s stopnjo tajnosti, ki ustreza stopnji tajnosti podatkov, do katerih naj bi imele dostop, in so ustrezno poučene.

3. Pogodbenici si medsebojno priznavata dovoljenja za dostop do tajnih podatkov za podatke stopnje SECRET/ZAUPNO in višje stopnje ali pisna pooblastila za podatke stopnje SECRET DE SERVICIU/INTERNO, kar omogoča dostop do tajnih podatkov v skladu z enakovrednimi oznakami stopnje tajnosti iz drugega odstavka 4. člena.

6. ČLEN

VAROVANJE TAJNIH PODATKOV

1. Pogodbenici zagotavljata tajnim podatkom iz tega sporazuma enako varovanje kot svojim podatkom z enakovredno stopnjo tajnosti.
2. Pogodbenica izvora obvešča pogodbenico prejemnico o pogojih za dajanje tajnih podatkov ali omejitvah pri njihovi uporabi in o vseh poznejših spremembah stopnje tajnosti.
3. Pogodbenica prejemnica zagotovi, da so tajni podatki označeni z enakovrednimi oznakami stopnje tajnosti skladno z drugim odstavkom 4. člena in da se stopnja tajnosti ne spremeni, zniža ali prekliče razen s pisnim dovoljenjem pogodbenice izvora.

7. ČLEN

OMEJITEV UPORABE TAJNIH PODATKOV

1. Pogodbenica prejemnica tajne podatke uporabi izključno za namen, za katerega so ji bili dani, in z omejitvami, ki jih je navedla pogodbenica izvora.
2. Pogodbenica prejemnica ne da tajnih podatkov tretji strani brez predhodnega pisnega soglasja pogodbenice izvora.

8. ČLEN

PRENOS TAJNIH PODATKOV

Prenos tajnih podatkov med pogodbenicama poteka po diplomatski ali vojaški poti ali po drugih poteh, o katerih se dogovorita pristojna nacionalna varnostna organa v skladu s svojo notranjo zakonodajo.

9. ČLEN

RAZMNOŽEVANJE, PREVAJANJE IN UNIČEVANJE TAJNIH PODATKOV

1. Vsi izvodi in prevodi imajo enako oznako stopnje tajnosti kakor tajni podatki izvirnika in so ustrezno varovani. Prevodi in število izvodov so omejeni na najmanjše število, potrebno za uradne namene.
2. Vsak prevod mora imeti v jeziku prevoda ustrezno navedbo, da vsebuje tajne podatke pogodbenice izvora, vključno z oznako stopnje tajnosti in številko izvirnika.
3. Tajni podatki z oznako STRICT SECRET DE IMPORTANTĂ DEOSEBITĂ/STROGO TAJNO se razmnožujejo izključno s pisnim dovoljenjem pogodbenice izvora.
4. Tajni podatki z oznako STRICT SECRET DE IMPORTANTĂ DEOSEBITĂ/STROGO TAJNO se ne smejo uničiti. Ko jih pogodbenica prejemnica ne potrebuje več, jih vrne pogodbenici izvora.
5. Ob neposredni nevarnosti se tajni podatki uničijo brez predhodnega dovoljenja. O tem se takoj uradno obvesti nacionalni varnostni organ pogodbenice izvora.
6. Tajni podatki stopnje STRICT SECRET/TAJNO ali nižje stopnje se, ko jih pogodbenica prejemnica ne potrebuje več, v skladu z njeno notranjo zakonodajo uničijo po predhodnem pisnem soglasju pogodbenice izvora.

10. ČLEN

POGODBE S TAJNIMI PODATKI

1. Preden se tajni podatki v zvezi s pogodbo s tajnimi podatki dajo izvajalcem ali podizvajalcem, nacionalni varnostni organ pogodbenice prejemnice:
 - a. potrdi, da imajo izvajalci ali podizvajalci, ki sodelujejo pri pogodbah s tajnimi podatki, ustrezno varnostno dovoljenje organizacije in da imajo njihovi zaposleni, ki sodelujejo pri pogodbah s tajnimi podatki, ustrezna dovoljenja za dostop do tajnih podatkov, ali

- b. na podlagi zaprosila začne v skladu z notranjo zakonodajo ustrezen postopek za izdajo potrebnih varnostnih dovoljenj organizacije ali dovoljenj za dostop do tajnih podatkov.
2. Nacionalni varnostni organ lahko zahteva varnostni pregled v organizaciji zaradi zagotavljanja stalnega upoštevanja varnostnih standardov v skladu z notranjo zakonodajo.
3. Pogodba s tajnimi podatki vsebuje prilogo z določbami o varnostnih zahtevah in stopnji tajnosti vsakega njenega vidika ali dela. Nacionalnima varnostnima organoma pogodbenic se predloži izvod take priloge.
4. Pogodbenici si medsebojno priznavata varnostna dovoljenja organizacije.

11. ČLEN

OBISKI

1. Za obiske, pri katerih je potreben dostop do tajnih podatkov, je potrebno predhodno dovoljenje nacionalnega varnostnega organa pogodbenice gostiteljice.
2. Zaposilo za obisk se predloži nacionalnemu varnostnemu organu vsaj 20 dni pred začetkom obiska ter vsebuje te osebne in druge podatke:
 - a. ime in priimek obiskovalca, datum in kraj rojstva, državljanstvo ter številko osebne izkaznice/potnega lista;
 - b. položaj obiskovalca s podatki o delodajalcu, ki ga obiskovalec zastopa;
 - c. opis dejavnosti, pri katerih obiskovalec sodeluje;
 - d. veljavnost in stopnjo tajnosti obiskovalčevega dovoljenja za dostop do tajnih podatkov, če se zahteva;
 - e. ime, naslov, telefonsko številko/številko telefaksa, elektronski naslov organizacije, v kateri bo obisk, in osebo za stike;
 - f. namen obiska, vključno z najvišjo stopnjo tajnosti tajnih podatkov, do katerih bo obiskovalec imel dostop;

- g. datum in trajanje obiska – pri večkratnih obiskih se navede celotno obdobje obiskov;
 - h. datum, podpis in žig nacionalnega varnostnega organa pogodbenice pošiljateljice.
3. V nujnih primerih se nacionalna varnostna organa lahko dogovorita za krajši rok predložitve zaprosila za obisk.
 4. Nacionalna varnostna organa se lahko dogovorita o seznamu obiskovalcev, ki imajo pravico do večkratnih obiskov. Seznam velja za začetno obdobje, ki ni daljše od 12 mesecev in se lahko podaljša za največ 12 mesecev. Zaposilo za večkratne obiske se predloži v skladu z drugim odstavkom. Ko je seznam potrjen, se lahko sodelujoči subjekti o obiskih dogovarjajo neposredno.
 5. Vsi tajni podatki, ki jih pridobi obiskovalec, veljajo za tajne podatke po tem sporazumu.
 6. Vsaka pogodbenica zagotavlja varstvo osebnih podatkov obiskovalcev v skladu s svojo notranjo zakonodajo.

12. ČLEN

SODELOVANJE PRI VAROVANJU TAJNOSTI

1. Zaradi doseganja in ohranjanja primerljivih varnostnih standardov se nacionalna varnostna organa na podlagi zaprosila obveščata o notranjih varnostnih standardih, postopkih in praksah za varovanje tajnih podatkov. V ta namen se lahko nacionalna varnostna organa obiskujeta.
2. Nacionalna varnostna organa se obveščata o varnostnih tveganjih, ki lahko ogrozijo izmenjane tajne podatke.
3. V skladu s svojimi pristojnostmi si lahko nacionalna varnostna organa na podlagi zaprosila pomagata pri izvajanju postopkov varnostnega preverjanja.
4. Nacionalna varnostna organa drug drugega takoj obvestita o vsaki spremembi pri medsebojno priznanih dovoljenjih za dostop do tajnih podatkov in varnostnih dovoljenjih organizacij.
5. Varnostne in obveščevalne službe pogodbenic si lahko v skladu z notranjo zakonodajo neposredno izmenjavajo operativne in/ali obveščevalne podatke.

13. ČLEN
OGROŽANJE TAJNIH PODATKOV

1. Pogodbenica takoj pisno obvesti drugo pogodbenico o sumu ali odkritju ogrožanja tajnih podatkov, izmenjanih po tem sporazumu.
2. Pogodbenica prejemnica sprejme vse mogoče ustrezne ukrepe v skladu s svojo notranjo zakonodajo, da omeji posledice ogrožanja in prepreči nadaljnje kršitve. Na podlagi zaprosila pogodbenica izvora pomaga pri preiskavi; pisno se obvesti o izidu preiskave in sprejetih ukrepih.

14. ČLEN
STROŠKI

Vsaka pogodbenica krije svoje stroške, ki nastanejo med izvajanjem tega sporazuma.

15. ČLEN
RAZLAGA IN REŠEVANJE SPOROV

Spore glede razlage ali uporabe tega sporazuma pogodbenici rešujeta izključno z medsebojnimi posvetovanji.

16. ČLEN
KONČNE DOLOČBE

1. Ta sporazum je sklenjen za nedoločen čas. Odobren mora biti v skladu z notranjepravnimi postopki pogodbenic in začne veljati prvi dan drugega meseca po prejemu zadnjega uradnega obvestila o tem, da so izpolnjene vse zahteve, potrebne za začetek veljavnosti tega sporazuma.
2. Ta sporazum se lahko kadar koli spremeni s pisnim soglasjem pogodbenic. Take spremembe začnejo veljati v skladu s prvim odstavkom.
3. Vsaka pogodbenica ima pravico, da ta sporazum kadar koli pisno odpove. V tem primeru sporazum preneha veljati 6 mesecev po dnevu, ko je druga pogodbenica prejela obvestilo o odpovedi sporazuma.

4. Ne glede na prenehanje veljavnosti tega sporazuma se vsi tajni podatki, izmenjani na njegovi podlagi, še naprej varujejo v skladu z njegovimi določbami, dokler pogodbenica izvora pogodbenice prejemnice ne razreši te obveznosti.
5. Za izvajanje sporazuma se lahko sklenejo dogovori o izvajanju.

V potrditev tega sta podpisana, ki sta bila za to pravilno pooblaščenata, podpisala ta sporazum.

Sestavljeno v Bukarešti dne 29. junija 2011 v dveh izvornikih v romunskem, slovenskem in angleškem jeziku, pri čemer so vsa besedila enako verodostojna. Pri različni razlagi prevlada angleško besedilo.

ZA VLADO ROMUNIJE
[Signature]

ZA VLADO REPUBLIKE
SLOVENIJE
[Signature]

[Signature]
[Signature]

AGREEMENT

BETWEEN

THE GOVERNMENT OF ROMANIA

AND

**THE GOVERNMENT OF THE REPUBLIC OF
SLOVENIA**

**ON THE MUTUAL PROTECTION
OF CLASSIFIED INFORMATION**

The Government of Romania
and
the Government of the Republic of Slovenia,
hereinafter referred to as the "Parties",

wishing to ensure the protection of Classified Information exchanged between
the Parties or between public and private entities subject to their respective
national legislation, taking into consideration national interests and security,

have agreed on the following:

ARTICLE 1

APPLICABILITY

1. This Agreement shall form the basis of any activity involving, in compliance with the national legislation of the Parties, the exchange of Classified Information between the Parties or other state bodies or public and private entities of their states.
2. This Agreement shall not affect the commitments of both Parties which stem from other international agreements and shall not be used against the interests, security and territorial integrity of other states.
3. In accordance with their national legislation both Parties shall take all appropriate measures to ensure the protection of Classified Information which is exchanged between them or generated under this Agreement.

ARTICLE 2

DEFINITIONS

For the purpose of this Agreement these terms mean the following:

- a) **Classified Information** means any information, regardless of its physical form, to which a classification level has been assigned in compliance with the national legislation and which shall be protected accordingly;
- b) **Classified Contract** means a contract, a subcontract or a project, including pre-contractual activities, which contains Classified Information or involves access to it;

- c) **Originating Party** means the Party, including any public or private entity subject to its national legislation, which generates and releases Classified Information to the Recipient Party;
- d) **Recipient Party** means the Party, including any public or private entity subject to its national legislation, which receives Classified Information from the Originating Party;
- e) **Third Party** means a state or any public or private entity or an international organisation, which is not a party to this Agreement;
- f) **Need-to-Know** means a principle by which access to Classified Information may be granted to an individual only in connection with his/her official duties or tasks;
- g) **Personnel Security Clearance Certificate** means a document, issued in accordance with the national legislation, certifying that the holder may access Classified Information of a certain security classification level;
- h) **Facility Security Clearance Certificate** means a document, issued in accordance with the national legislation, certifying that a legal entity fulfils the conditions for handling classified information of a specific classification level and is authorised to perform activities related to a classified contract;
- i) **Compromise of Classified Information** means a situation when, due to a breach of security, Classified Information has lost its confidentiality, integrity or availability.

ARTICLE 3

COMPETENT SECURITY AUTHORITIES

1. The National Security Authorities designated by the Parties as responsible for the general implementation and the relevant controls of all aspects of this Agreement are:

In Romania:

Oficiul Registrului Național al Informațiilor Secrete de Stat

In the Republic of Slovenia:

Urad Vlade Republike Slovenije za varovanje tajnih podatkov

2. The National Security Authorities shall notify each other of any other competent security authorities that are responsible for the implementation of this Agreement.
3. The Parties shall inform each other of any subsequent changes of the National Security Authorities.

ARTICLE 4

SECURITY CLASSIFICATIONS

1. Classified Information released under this Agreement shall be marked with the appropriate classification level under the national legislation of each of the Parties.
2. The equivalence of the national classification markings is as follows:

Romania	Republic of Slovenia
STRICT SECRET DE IMPORTANȚĂ DEOSEBITĂ	STROGO TAJNO
STRICT SECRET	TAJNO
SECRET	ZAUPNO
SECRET DE SERVICIU	INTERNO

ARTICLE 5

ACCESS TO CLASSIFIED INFORMATION

1. Access to information classified SECRET DE SERVICIU/INTERNO shall be limited to persons who have been granted such access according to the national legislation, have a Need-to-Know, and have been briefed accordingly.
2. Access to information classified SECRET/ZAUPNO and above shall be limited to persons who have a Need-to-Know and who, in accordance with the national legislation, have been issued a Personnel Security Clearance Certificate corresponding to the classification level of the information to be accessed, and have been briefed accordingly.

3. The Parties shall mutually recognise their respective Personnel Security Clearance Certificates for information classified SECRET/ZAUPNO and above or written authorisations for information classified SECRET DE SERVICIU/INTERNO, which shall enable access to Classified Information according to the equivalence stated in Paragraph 2 of Article 4.

ARTICLE 6

PROTECTION OF CLASSIFIED INFORMATION

1. The Parties shall afford the same protection to Classified Information referred to in this Agreement as to their own information of the corresponding classification level.
2. The Originating Party shall inform the Recipient Party of any conditions of release or limitations on the use of Classified Information, and of any subsequent changes in the classification level.
3. The Recipient Party shall ensure that Classified Information is marked with an equivalent classification level in accordance with Paragraph 2 of Article 4, and that the classification level is not changed, downgraded, or declassified unless authorised in writing by the Originating Party.

ARTICLE 7

RESTRICTION OF USE OF CLASSIFIED INFORMATION

1. The Recipient Party shall use Classified Information only for the purpose for which it has been released and within the limitations stated by the Originating Party.
2. The Recipient Party shall not release Classified Information to a Third Party without the prior written consent of the Originating Party.

ARTICLE 8

TRANSMISSION OF CLASSIFIED INFORMATION

Classified Information shall be transmitted between the Parties through diplomatic or military channels or through other channels agreed upon by the National Security Authorities in accordance with the respective national legislation.

ARTICLE 9

REPRODUCTION, TRANSLATION AND DESTRUCTION OF CLASSIFIED INFORMATION

1. All reproductions and translations shall bear the same classification markings as the original Classified Information and shall be protected accordingly. The translations and the number of reproductions shall be limited to the minimum required for an official purpose.
2. All translations shall contain a suitable annotation, in the language of translation, indicating that they contain Classified Information of the Originating Party, including classification marking and the reference number of the original document.
3. Classified Information marked STRICT SECRET DE IMPORTANTĂ DEOSEBITĂ/STROGO TAJNO shall be reproduced only upon the written permission of the Originating Party.
4. Classified Information marked STRICT SECRET DE IMPORTANTĂ DEOSEBITĂ/STROGO TAJNO shall not be destroyed. It shall be returned to the Originating Party after it is no longer considered necessary by the Recipient Party.
5. In case of an imminent danger, Classified Information shall be destroyed without prior authorisation. The National Security Authority of the Originating Party shall immediately be notified of this.
6. Information classified STRICT SECRET/TAJNO or below shall be destroyed after it is no longer considered necessary by the Recipient Party, in accordance with its national legislation, with the prior written consent of the Originating Party.

ARTICLE 10

CLASSIFIED CONTRACTS

1. Before providing Classified Information related to a Classified Contract to contractors or sub-contractors, the National Security Authority of the Recipient Party shall:

- a. confirm that contractors or sub-contractors participating in Classified Contracts have appropriate Facility Security Clearance Certificates, and their employees involved in Classified Contracts have appropriate Personnel Security Clearance Certificates; or
 - b. initiate upon request the appropriate procedure in accordance with the national legislation, in order to issue the relevant Facility Security Clearance Certificates or Personnel Security Clearance Certificates.
2. Either of the National Security Authorities may request that a security inspection is carried out at a facility to ensure continuing compliance with security standards in accordance with the national legislation.
 3. A Classified Contract shall contain an annex with provisions on the security requirements and the classification of each aspect or element of the Classified Contract. A copy of such annex shall be submitted to the National Security Authorities of the Parties.
 4. The Parties shall mutually recognise their respective Facility Security Clearance Certificates.

ARTICLE 11

VISITS

1. Visits necessitating access to Classified Information shall be subject to the prior permission of the National Security Authority of the host Party.
2. A request for visit shall be submitted to the National Security Authority at least 20 days prior to the commencement of the visit and shall include the following personal and other data:
 - a. The visitor's name, date and place of birth, nationality and ID card/passport number;
 - b. The visitor's position, with a specification of the employer which the visitor represents;
 - c. A specification of the activities in which the visitor participates;
 - d. The validity and level of the visitor's Personnel Security Clearance Certificate, if required;

- e. The name, address, phone/fax number, e-mail and point of contact at the facility to be visited;
 - f. The purpose of the visit, including the highest level of Classified Information to be accessed;
 - g. The date and duration of the visit – in the case of recurring visits the total period covered by the visits shall be stated;
 - h. The date, signature and stamp of the National Security Authority of the sending Party.
3. In urgent cases, the National Security Authorities may agree on a shorter period for the submission of the request for visit.
 4. The National Security Authorities may agree on a list of visitors entitled to recurring visits. This list shall be valid for an initial period not exceeding 12 months and may be extended for a further period of time not exceeding 12 months. A request for recurring visits shall be submitted in accordance with Paragraph 2. Once the list has been approved, visits may be arranged directly between the entities involved.
 5. Any Classified Information acquired by a visitor shall be considered as Classified Information under this Agreement.
 6. Each Party shall guarantee the protection of the personal data of the visitors according to its national legislation.

ARTICLE 12

SECURITY CO-OPERATION

1. In order to achieve and maintain comparable standards of security, the National Security Authorities shall, upon request, provide each other with information concerning their national security standards, procedures and practices for the protection of Classified Information. To this end the National Security Authorities may visit each other.
2. The National Security Authorities shall inform each other of security risks that may endanger the exchanged Classified Information.

3. On request, the National Security Authorities may, in accordance with their powers, assist each other in carrying out security clearance procedures.
4. The National Security Authorities shall promptly inform each other of any changes in mutually recognised Personnel Security Clearance Certificates and Facility Security Clearance Certificates.
5. The security and intelligence services of the Parties may exchange operative and/or intelligence information directly in accordance with national legislation.

ARTICLE 13

COMPROMISE OF CLASSIFIED INFORMATION

1. Each Party shall immediately notify the other Party in writing of any suspicion or discovery of a compromise of Classified Information exchanged under this Agreement.
2. The Recipient Party shall undertake all possible appropriate measures under its national legislation so as to limit the consequences of the compromise and to prevent further violations. On request, the Originating Party shall provide investigative assistance; it shall be informed in writing of the outcome of the investigation and the measures undertaken.

ARTICLE 14

EXPENSES

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

ARTICLE 15

INTERPRETATION AND DISPUTE SETTLEMENT

Any dispute between the Parties on the interpretation or application of this Agreement shall be resolved exclusively by means of consultation between the Parties.

ARTICLE 16
FINAL PROVISIONS

1. This Agreement is concluded for an indefinite period of time. It is subject to approval in accordance with the national legal procedures of the Parties and shall enter into force on the first day of the second month following the receipt of the last notification that the necessary requirements for this Agreement to enter into force have been met.
2. This Agreement may be amended at any time by the written consent of both Parties. Such amendments shall enter into force in accordance with Paragraph 1.
3. Each Party has the right to terminate this Agreement in writing at any time. In such a case the validity of the Agreement shall expire 6 months following the day on which the termination notice was received by the other Party.
4. Notwithstanding the termination of this Agreement, all Classified Information exchanged under this Agreement shall continue to be protected in accordance with the provisions stated in this Agreement until the Originating Party dispenses the Recipient Party from this obligation.
5. Implementing arrangements may be concluded for the implementation of this Agreement.

In witness whereof the undersigned, being duly authorised thereto, have signed this Agreement.

Done at Bucharest on 29th June 2011 in two originals in the Romanian, Slovenian and English languages, each text being equally authentic. In case of different interpretation, the English text shall prevail.

**ON BEHALF OF
THE GOVERNMENT OF
ROMANIA**

[Handwritten signature]

**ON BEHALF OF
THE GOVERNMENT OF THE
REPUBLIC OF SLOVENIA**

[Handwritten signature]

*Conform cu originalul
[Handwritten signature]*