

ACORD

ÎNTRE

GUVERNUL ROMÂNIEI

ȘI

GUVERNUL REPUBLICII BULGARIA

PRIVIND PROTECȚIA RECIPROCĂ

A INFORMAȚIILOR CLASIFICATE



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

Cunoscând faptul că buna cooperare poate face necesar un schimb de Informații Clasificate între Părțile Contractante,

Dorind să stabilească un set de reguli care să reglementeze protecția reciprocă a Informațiilor Clasificate ce se vor aplica tuturor acordurilor de cooperare și Contractelor Clasificate viitoare ce vor fi stabilite între Părțile Contractante și care vor conține și implica accesul la Informații Clasificate,

Au convenit următoarele:

ARTICOLUL 1 DISPOZIȚII GENERALE

(1) Prezentul Acord va sta la baza tuturor activităților ce implică, în conformitate cu legislațiile naționale, schimbul de Informații Clasificate între Părțile Contractante, direct sau prin intermediul altor organisme de stat sau persoane juridice.

(2) Decizia privind schimbul de Informații Clasificate între Părțile Contractante se ia în conformitate cu legislațiile naționale ale acestora.

(3) Părțile Contractante își vor îndeplini obligațiile stipulate în prezentul Acord, conform condițiilor stabilite prin acesta, pe baza principiilor egalității și avantajului reciproc.

(4) Prezentul Acord nu va afecta obligațiile celor două Părți Contractante ce derivă din alte acorduri internaționale și 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, indiferent de forma sa fizică, căreia i s-a atribuit un nivel de clasificare de securitate în conformitate cu legislațiile naționale și care va fi protejată în mod corespunzător;

b) **Document Clasificat** înseamnă:

orice Informație Clasificată înregistrată, indiferent de forma și caracteristicile sale fizice, incluzând, dar fără a se limita la, următoarele suporturi relevante: hârtie scrisă de mână sau imprimată, sigilii, aplicații utilizate pentru procesarea datelor, hărți, tabele, fotografii, imagini, litografii, gravuri, desene sau părți din acestea, schițe, ciorne, note, foi de indigo, riboane de tipărit sau pentru multiplicarea efectuată prin orice mijloace ori procese, înregistrări audio, vocale, magnetice ori video, electronice sau optice sub orice formă, cât și echipamente portabile de procesare automată a datelor cu medii de stocare fixe sau detașabile;

c) **Material Clasificat** înseamnă:

orice articol tehnic, prototip, echipament, instalație, dispozitiv sau armă fabricat sau în curs de fabricație, precum și componentele folosite la fabricarea acestora, ce conțin Informații Clasificate;

d) **Marcajul Clasificării de Securitate** înseamnă:

un marcaj ce indică nivelul clasificării de securitate a Informației Clasificate, în conformitate cu legislațiile din statele Părților Contractante;

e) **Contract sau Sub-contract Clasificat** înseamnă:

un acord încheiat în conformitate cu legislațiile naționale, între Contractanți sau între Contractanți și Sub-contractanți, care conține și/ sau implică acces la Informații Clasificate în procesul derulării sale;

f) **Contractant sau Sub-contractant** înseamnă:

o persoana fizică sau juridică ce are capacitatea legală de a încheia Contracte Clasificate sau care este parte la un Contract Clasificat;



g) Incident de Securitate înseamnă:
o acțiune sau inacțiune contrară legislației naționale care are sau poate avea ca rezultat Accesul Neautorizat la Informații Clasificate;

h) Accesul Neautorizat la Informații Clasificate înseamnă:
dezvăluirea, utilizarea greșită, modificarea, deteriorarea, prezentarea, distrugerea neautorizată a Informațiilor Clasificate, precum și orice alte acte ce duc la încălcarea măsurilor de protecție sau la pierderea unor astfel de informații;

i) Certificat de Securitate înseamnă:
o decizie pozitivă ca urmare a unei proceduri de vetting care va atesta loialitatea și onestitatea unei persoane și va dovedi conformitatea cu condițiile stipulate în legislația națională. Pe baza acestei decizii pozitive se poate acorda unei astfel de persoane accesul la informații cu un anumit nivel de clasificare;

j) Certificat de Securitate Industrială înseamnă:
o decizie pozitivă ca urmare a unei proceduri de vetting care va atesta capacitatea fizică și organizatorică a unei persoane juridice de a proteja corespunzător Informațiile Clasificate și care va dovedi conformitatea cu condițiile stipulate în reglementările naționale. Pe baza acestei decizii pozitive, unei astfel de persoane juridice i se poate acorda accesul la informații cu un anumit nivel de clasificare;

k) Principiul „Necesitatea de a Cunoaște” înseamnă:
un principiu potrivit căruia accesul la Informații Clasificate se va acorda doar acelei persoane care, în executarea sarcinilor sau atribuțiilor sale oficiale, necesită accesul la astfel de informații;

l) Autoritatea Competentă de Securitate înseamnă:
autoritatea care, conform legislației naționale a statului Părții Contractante respective, aplică politica aceluși stat în domeniul protecției Informațiilor Clasificate, exercită controlul general în această sferă de activitate și răspunde de implementarea prezentului Acord, fiind stabilită ca atare în art. 4 din prezentul Acord;

m) Autoritate Specializată de Securitate înseamnă:
instituția care, conform legislației naționale, are competențe specifice în domeniul protecției Informațiilor Clasificate;



n) **Tert** înseamnă:

un stat sau o organizație internațională, care nu este parte la prezentul Acord sau o persoană fizică ori juridică ce nu îndeplinește cerințele naționale respective privind accesul la Informații Clasificate, inclusiv principiul „Necesității de a Cunoaște”.

ARTICOLUL 3 NIVELURILE CLASIFICĂRILOR DE SECURITATE

(1) Nivelurile clasificărilor de securitate ce se aplică informațiilor schimbate în cadrul prezentului Acord sunt:

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

b) pentru Republica Bulgaria: СТРОГО СЕКРЕТНО (TOP SECRET), СЕКРЕТНО (SECRET), ПОВЕРИТЕЛНО (CONFIDENTIAL) și ЗА СЛУЖЕБНО ПОЛЗВАНЕ (RESTRICTED).

(2) Părțile Contractante au stabilit echivalența nivelurilor clasificărilor de securitate după cum urmează:

România	Bulgaria	Echivalentul în limba engleză
STRICT SECRET DE IMPORTANTĂ DEOSEBITĂ	СТРОГО СЕКРЕТНО	TOP SECRET
STRICT SECRET	СЕКРЕТНО	SECRET
SECRET	ПОВЕРИТЕЛНО	CONFIDENTIAL
SECRET DE SERVICIU	ЗА СЛУЖЕБНО ПОЛЗВАНЕ	RESTRICTED

(3) Numai Partea Contractantă emitentă este autorizată să modifice nivelul clasificării de securitate sau să declassifice Informațiile Clasificate transmise. Atribuirea unui nivel de clasificare de securitate Informațiilor Clasificate stabilite în comun, modificarea acestuia sau declassificarea acestor informații se vor face prin acordul Părților Contractante.

ARTICOLUL 4 AUTORITĂȚILE COMPETENTE DE SECURITATE

(1) Autoritățile Competente de Securitate responsabile de implementarea și controlul corespunzător al tuturor aspectelor prezentului Acord sunt:

- **În România:** Guvernul României, Oficiul Registrului Național al Informațiilor Secrete de Stat - ORNISS, (Government of Romania, National Registry Office for Classified Information), București, str. Mureș nr. 4, sector 1 ROMÂNIA;

- **În Republica Bulgaria:** Държавна Комисия по Сигурността на Информацията – ДКСИ, София, Ул. Ангел Кънчев, 1, БЪЛГАРИЯ (State Commission on Information Security), Sofia, str. Angel Kanchev nr.1, BULGARIA.

(2) În vederea realizării și menținerii unor standarde comparabile de securitate, Autoritățile Competente de Securitate își vor furniza reciproc, la cerere, informații despre standardele, procedurile și practicile de securitate pentru protecția Informațiilor Clasificate, aplicate de către Partea Contractantă respectivă. Autoritățile Competente de Securitate vor permite, de comun acord, efectuarea de vizite de inspecție în ambele țări, de către persoane oficiale autorizate.

ARTICOLUL 5 MĂSURI DE PROTECȚIE A INFORMAȚIILOR CLASIFICATE

(1) În conformitate cu prezentul Acord și legislațiile naționale, Părțile Contractante vor implementa toate măsurile corespunzătoare pentru protecția Informațiilor Clasificate care sunt schimbate sau produse conform prezentului Acord. Acestor Informații Clasificate li se va asigura același nivel de protecție ca și Informațiilor Clasificate naționale, cu un nivel de clasificare de securitate corespunzător, conform art. 3.

(2) Partea Contractantă primitoare nu va utiliza un nivel de clasificare inferior pentru Informațiile Clasificate primite și nici nu va declassifica aceste



informații fără acordul prealabil scris al Autorității Competente de Securitate a Părții Contractante emitente.

(3) Partea Contractantă primitoare este obligată:

a) să nu dezvăluie Informații Clasificate unui Terț fără acordul prealabil scris al Părții Contractante emitente;

b) să atribuie Informațiilor Clasificate un nivel de clasificare de securitate echivalent cu cel atribuit de Partea Contractantă emitentă;

c) să nu utilizeze Informațiile Clasificate în alte scopuri decât cele pentru care au fost furnizate;

d) să garanteze drepturile civile precum drepturile de brevet, drepturile de autor sau secretele comerciale cuprinse în Informații Clasificate.

(4) Partea Contractantă emitentă se va asigura că Partea Contractantă primitoare este informată asupra:

a) Marcajelor Clasificărilor de Securitate ale informațiilor și a tuturor condițiilor de diseminare sau limitare a utilizării lor și asupra faptului că informațiile sunt marcate corespunzător;

b) oricăror modificări ulterioare ale nivelurilor clasificărilor de securitate.

(5) În cazul în care orice alt acord încheiat între Părțile Contractante conține reglementări mai stricte privind schimbul sau protecția Informațiilor Clasificate, se vor aplica respectivele reglementări.

(6) În cazul în care sunt imposibile protejarea și returnarea Informațiilor Clasificate produse sau schimbate conform prezentului Acord, Informațiile Clasificate vor fi distruse imediat. Partea Contractantă primitoare va informa imediat Autoritatea Competentă de Securitate a Părții Contractante emitente asupra distrugerii Informațiilor Clasificate.



ARTICOLUL 6

TRANSMITEREA INFORMAȚIILOR CLASIFICATE

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

(2) Dacă există un volum mare de Informații Clasificate ce trebuie transmis, Autoritățile Competente de Securitate vor conveni și vor aproba de comun acord modalitățile de transport, ruta și măsurile de securitate pentru fiecare caz în parte.

(3) Schimbul de Informații Clasificate prin intermediul sistemelor informatice și de comunicații se realizează conform procedurilor de securitate stabilite în legislația națională.

ARTICOLUL 7

MARCAJELE CLASIFICĂRILOR DE SECURITATE

(1) Partea Contractantă primitoare va marca Informațiile Clasificate ale Părții Contractante emitente cu Marcaje ale Clasificării de Securitate echivalente, în conformitate cu art. 3 din prezentul Acord.

(2) Informațiile Clasificate produse în comun vor fi marcate de către Partea Contractantă pe teritoriul căreia acestea au fost produse. În acest caz, această Parte Contractantă va fi considerată Parte Contractantă emitentă. Partea Contractantă emitentă poate transmite Informațiile Clasificate produse în comun către un Terț numai cu acordul prealabil scris al celeilalte Părți Contractante.

(3) Informațiile Clasificate produse de către Partea Contractantă primitoare pe baza Informațiilor Clasificate sau a unei părți din Informațiile Clasificate transmise de Partea Contractantă emitentă vor fi marcate cu Marcaje de Clasificare de Securitate, ce nu vor fi inferioare Marcajelor Clasificărilor de Securitate ale Informațiilor Clasificate transmise.



ARTICOLUL 8

TRADUCEREA, MULTIPLICAREA, DISTRUGEREA

(1) Documentele Clasificate marcate cu nivelul de clasificare de securitate STRICT SECRET DE IMPORTANTĂ DEOSEBITĂ / СТРОГО СЕКРЕТНО / TOP SECRET vor fi traduse sau copiate numai cu acordul scris al Autorității Competente de Securitate a Părții Contractante emitente.

(2) Orice traducere a Informațiilor Clasificate va purta Marcajul de Clasificare de Securitate a originalului și o adnotare corespunzătoare în limba în care au fost traduse, ce va indica faptul că materialul tradus conține Informații Clasificate ale Părții Contractante emitente.

(3) În cazul în care Informațiile Clasificate sunt multiplicare sau copiate, toate Marcajele Clasificărilor de Securitate de pe original vor fi multiplicare sau marcate pe fiecare copie. Astfel de informații multiplicare sau copiate vor fi supuse aceluiași măsuri de protecție ca și informațiile originale. Numărul de copii se va limita la cel necesar scopurilor oficiale.

(4) Informațiile Clasificate vor fi distruse sau modificate astfel încât să se împiedice reconstituirea lor totală sau parțială.

(5) Informațiile Clasificate cu nivelul de clasificare de securitate STRICT SECRET DE IMPORTANTĂ DEOSEBITĂ / СТРОГО СЕКРЕТНО / TOP SECRET nu vor fi distruse. Acestea vor fi returnate Părții Contractante emitente.

(6) Partea Contractantă emitentă poate interzice în mod expres multiplicarea, modificarea sau distrugerea unei Informații Clasificate prin marcarea suportului relevant al Informației Clasificate sau prin trimiterea în acest sens a unei înștiințări scrise. În acest caz, respectivele Informații Clasificate vor fi returnate Părții Contractante emitente, cu excepția menționată la art. 5, alin. (6).



ARTICOLUL 9 CERTIFICATELE DE SECURITATE

(1) Fiecare Parte Contractantă va garanta că toate persoanele care, prin natura sarcinilor și îndatoririlor de serviciu necesită acces la Informații Clasificate, dețin Certificate de Securitate valabile și corespunzătoare, emise în conformitate cu legislația națională.

(2) La cerere, Autoritățile Competente de Securitate / Autoritățile Specializate de Securitate ale Părților Contractante, în conformitate cu legislația națională, vor face schimb de informații referitoare la persoanele fizice sau juridice verificate.

(3) La cerere, Autoritatea Competentă de Securitate a fiecărei Părți Contractante va oferi informații privind emiterea pentru o persoană fizică sau juridică a unui Certificat de Securitate/ Certificat de Securitate Industrială național care să corespundă nivelului de clasificare de securitate solicitat.

Dacă o persoană fizică sau juridică nu deține Certificat de Securitate/ Certificat de Securitate Industrială, Autoritatea Competentă de Securitate a fiecărei Părți Contractante poate solicita verificarea de securitate pentru acea persoană fizică sau juridică.

(4) Părțile Contractante vor recunoaște reciproc valabilitatea Certificatelor de Securitate/ Certificatelor de Securitate Industrială în conformitate cu legislația națională.

(5) Autoritățile Competente de Securitate se vor înștiința reciproc asupra oricăror situații de retragere sau scădere a nivelului Certificatelor de Securitate/Certificatelor de Securitate Industrială emise persoanelor fizice sau juridice care desfășoară activități conform prevederilor prezentului Acord.

ARTICOLUL 10 SECURITATEA INDUSTRIALĂ

(1) Contractele Clasificate vor fi încheiate și implementate în conformitate cu legislațiile naționale ale Părților Contractante și cu prevederile prezentului Acord.



(2) În cazul în care un Contract Clasificat se derulează pe teritoriul statului uneia dintre Părțile Contractante, autoritățile din statul acelei Părți Contractante sunt obligate să exercite controlul privind îndeplinirea de către Contractant a obligațiilor de protecție a Informațiilor Clasificate.

(3) Înainte de transmiterea către Contractanții din statul fiecărei Părți Contractante a unor Informații Clasificate ale celeilalte Părți Contractante, Partea Contractantă primitoare:

a) va acorda Contractanților Certificate de Securitate Industrială corespunzătoare, cu condiția ca aceștia să îndeplinească cerințele pentru emiterea lui;

b) va acorda Certificate de Securitate corespunzătoare tuturor persoanelor care, prin natura sarcinilor și îndatoririlor de serviciu necesită acces la Informații Clasificate, cu condiția ca acestea să îndeplinească cerințele pentru emiterea lui;

c) se va asigura că toate persoanele care au acces la Informațiile Clasificate primite au fost corespunzător instruite asupra procedurilor și obligațiilor de securitate. Toate persoanele instruite vor declara în scris că înțeleg pe deplin responsabilitățile ce le revin și consecințele prevăzute de legislația națională pentru situațiile în care Informațiile Clasificate ajung în posesia unor persoane neautorizate, fie intenționat, fie din neglijență.

(4) Fiecare Contract Clasificat va cuprinde o Anexă de Securitate corespunzătoare. Anexa de Securitate va specifica informațiile referitoare la diferite aspecte din Contractul Clasificat care necesită protecție și nivelul de clasificare de securitate ce urmează a fi atribuit, precum și cerințele de securitate ce trebuie îndeplinite.

(5) Contractele Clasificate care implică Informații Clasificate de nivel SECRET DE SERVICIU /ЗА СЛУЖЕБНО ПОЛЗБАHE /RESTRICTED vor conține o clauză corespunzătoare care să specifice măsurile minime ce se vor implementa pentru protecția unor astfel de Informații Clasificate.



ARTICOLUL 11 VIZITE

(1) Vizitele în obiective unde se elaborează, se gestionează sau stochează Informații Clasificate vor fi permise vizitatorilor din statul celeilalte Părți Contractante, dacă aceștia necesită acces la Informații Clasificate, numai de către Autoritatea Competentă de Securitate a statului vizitat.

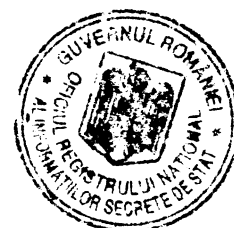
(2) Fiecare Parte Contractantă va înștiința în timp util cealaltă Parte Contractantă asupra vizitatorilor așteptați înainte de vizita planificată. În cazurile urgente în care vizitele nu pot fi anunțate în timp util, se pot aranja vizite prin măsuri speciale stabilite de comun acord.

(3) Partea Contractantă gazdă va răspunde de informarea în mod expres a personalului din incintele și clădirile ce urmează a fi vizitate în legătură cu deciziile referitoare la obiectivul vizitei și cu nivelul maxim de clasificare a Informațiilor Clasificate ce urmează a fi puse la dispoziția Părții Contractante oaspete.

(4) Cererea privind efectuarea vizitei va fi înaintată în scris Autorității Competente de Securitate a Părții Contractante din statul al cărui teritoriu va fi vizitat.

(5) Cererea de vizită va conține următoarele informații:

- numele vizitatorului propus, data și locul nașterii, naționalitatea și numărul pașaportului (cărții de identitate);
- calitatea oficială a vizitatorului, precum și denumirea instituției, companiei sau organizației pe care o reprezintă sau din care face parte;
- menționarea nivelului Certificatului de Securitate al vizitatorului;
- denumirea și adresa instituției, companiei sau organizației care urmează a fi vizitată;
- numele și funcția persoanei/ persoanelor ce urmează fi vizitate, dacă sunt cunoscute;



- scopul vizitei;
- data sosirii și plecării.

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

(7) Toți vizitatorii vor respecta legislația națională privind protecția Informațiilor Clasificate a Părții Contractante gazde.

ARTICOLUL 12 INCIDENTELE DE SECURITATE

(1) În cazul producerii unui Incident de Securitate, Autoritatea Competentă de Securitate din statul în care s-a produs Incidentul de Securitate va informa imediat Autoritatea Competentă de Securitate din statul celeilalte Părți Contractante, va asigura investigația adecvată a acestui caz și va lua măsurile necesare de limitare a daunelor în conformitate cu legislația națională. Dacă vor fi solicitate, autoritățile din statul celeilalte Părți Contractante vor coopera la investigație.

(2) În cazul unui Incident de Securitate produs într-un stat terț, Autoritatea Competentă de Securitate a Părții Contractante care a transmis informațiile către statul terț va acționa, dacă este posibil, conform celor menționate la alin. (1).

(3) Autoritatea Competentă de Securitate a statului în care s-a produs Incidentul de Securitate va informa în scris cealaltă Parte Contractantă despre rezultatul investigației cu privire la cauzele evenimentului, gravitatea prejudiciului și măsurile întreprinse pentru limitarea și pentru prevenirea repetării acestuia.

ARTICOLUL 13 SOLUȚIONAREA DIFERENDELOR

Orice divergență privind interpretarea sau aplicarea prezentului Acord va fi soluționată prin consultare între Autoritățile Competente de Securitate din cele două state, fără a recurge la o jurisdicție străină.



ARTICOLUL 14 CHELTUIELI

Fiecare Parte Contractantă va suporta cheltuielile proprii survenite pe parcursul implementării prezentului Acord.

ARTICOLUL 15 ASISTENȚA RECIPROCĂ

(1) Fiecare Parte Contractantă și autoritățile din statul acesteia cu atribuții în domeniul protecției informațiilor clasificate, potrivit legislației naționale, vor acorda asistență personalului din statul celeilalte Părți Contractante în îndeplinirea obligațiilor și exercitarea drepturilor, în conformitate cu prevederile prezentului Acord.

(2) Dacă va fi cazul, Autoritățile Competente de Securitate ale Părților Contractante se vor consulta reciproc asupra unor aspecte tehnice concrete privind implementarea prezentului Acord.

(3) Autoritățile Competente de Securitate își vor furniza reciproc informațiile necesare aplicării dispozițiilor prezentului Acord.

ARTICOLUL 16 DISPOZIȚII FINALE

(1) Prezentul Acord este încheiat pe o perioadă nedeterminată și intră în vigoare la data primirii ultimei notificări prin care părțile se informează reciproc cu privire la îndeplinirea tuturor procedurilor interne necesare pentru intrarea sa în vigoare.

(2) Prezentul Acord poate fi amendat și completat pe baza consimțământului reciproc al celor două Părți Contractante. Asemenea amendamente sau completări vor fi făcute în scris și vor intra în vigoare în conformitate cu prevederile alin. (1).



(3) Fiecare Parte Contractantă are dreptul să denunțe oricând prezentul Acord, în scris. În acest caz, valabilitatea Acordului va expira după 6 (șase) luni de la data primirii de către cealaltă Parte Contractantă a notificării denunțării.

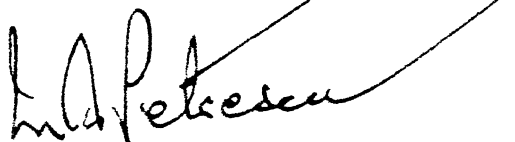
(4) În cazul încetării valabilității prezentului Acord, toate Informațiile Clasificate furnizate în baza acestui Acord vor continua să fie protejate conform prevederilor acestuia, până când Partea Contractantă emitentă absolvă de această obligație Partea Contractantă primitoare.

(5) Fiecare Parte Contractantă va notifica fără întârziere cealaltă Parte Contractantă asupra oricăror modificări intervenite în legislația națională care ar putea afecta protecția Informațiilor Clasificate asigurată prin prezentul Acord. În acest caz, Părțile Contractante se vor consulta pentru a analiza posibilele modificări ale prezentului Acord. Între timp, Informațiile Clasificate vor continua să fie protejate conform prevederilor acestuia.

(6) La data intrării în vigoare a prezentului Acord, Acordul dintre Guvernul României și Guvernul Republicii Bulgaria privind protecția informațiilor militare secrete schimbate, semnat la Sofia, la 29 martie 2000 își încetează valabilitatea.

Semnat la București, la 13 aprilie 2006, în două exemplare originale, fiecare în limbile română, bulgară și engleză, toate textele fiind egal autentice. În cazul unor diferențe de interpretare, va prevala textul în limba engleză.

**PENTRU
GUVERNUL ROMÂNIEI**



Prof. dr. MARIUS PETRESCU
Secretar de Stat
Directorul General
al Oficiului Registrului Național
al Informațiilor Secrete de Stat

**PENTRU
GUVERNUL REPUBLICII
BULGARIA**



TSVETA MARKOVA
Președintele
Comisiei de Stat pentru Securitatea
Informațiilor



СПОРАЗУМЕНИЕ

МЕЖДУ

ПРАВИТЕЛСТВОТО НА РУМЪНИЯ

И

ПРАВИТЕЛСТВОТО НА РЕПУБЛИКА БЪЛГАРИЯ

ЗА ВЗАИМНА ЗАЩИТА

НА

КЛАСИФИЦИРАНА ИНФОРМАЦИЯ



Правителството на Румъния и Правителството на Република България, наричани по-нататък Договарящи страни,

Разбирайки, че при ползотворното сътрудничество е възможно да се наложи обмен на класифицирана информация между Договарящите страни,

Желаейки да създадат правила, регулиращи взаимната защита на класифицирана информация, които ще се прилагат спрямо последващи споразумения за сътрудничество и класифицирани договори, които ще се изпълняват от Договарящите страни, съдържащи класифицирана информация или предполагащи достъп до класифицирана информация,

се договориха за следното:

ЧЛЕН 1 ОБЩИ ПОЛОЖЕНИЯ

(1) Това Споразумение формира основата на всяка дейност, включваща в съответствие с националното законодателство обмен на класифицирана информация между Договарящите страни пряко или чрез други държавни органи или юридически лица.

(2) Решението относно обмена на класифицирана информация между Договарящите страни се взема в съответствие с тяхното национално законодателство.

(3) Договарящите страни изпълняват задълженията си, посочени в това Споразумение в съответствие с неговите разпоредби, на основата на равноправието и взаимната изгода.

(4) Това Споразумение не засяга задълженията на двете Договарящи страни, произтичащи от други международни споразумения и не може да бъде използвано срещу интересите, сигурността и териториалната цялост на други държави.



ЧЛЕН 2 ОПРЕДЕЛЕНИЯ

За целите на това Споразумение:

а) **“Класифицирана информация”** означава: всяка информация, независимо от физическата ѝ форма, на която е определено ниво на класификация за сигурност в съответствие с националното законодателство и която следва да се защитава съответно;

б) **“Класифициран документ”** означава: всякакъв вид запис, съдържащ класифицирана информация, независимо от неговата физическа форма или характеристики, включително следните носители на информация, без изброяването да е изчерпателно: ръчно или машинно написан материал, програми за обработка на данни, карти, таблици, снимки, картини, оцветявания, гравюри, рисунки или части от тях, скици, чернови, работни бележки, индигов лист, мастилени ленти или възпроизвеждане чрез каквито и да е средства или процеси на звук, глас, магнитни записи, видеозаписи, електронни записи или оптични записи, в каквато и да е форма, както и преносимо оборудване за автоматизирана обработка на данни с постоянен или с преносим носител на информация;

в) **“Класифициран материал”** означава: всеки предмет от техническо естество, прототип, оборудване, инсталация, устройство или оръжие, произведени или в процес на производство, както и елементите, използвани за тяхното производство, съдържащи класифицирана информация;

г) **“Гриф за сигурност”** означава маркировка, която показва нивото на класификация за сигурност на класифицирана информация, в съответствие с националните законодателства на държавите на Договарящите страни;

д) **“Класифициран договор или договор с под-изпълнител”** означава: споразумение, сключено в съответствие с националното законодателство, между контрагенти или между контрагент и под-



изпълнител, съдържащо и/или предполагащо достъп до класифицирана информация в процеса на неговото изпълнение;

е) **“Контрагент или под-изпълнител”** означава:

физическо или юридическо лице, притежаващо правоспособност да сключва класифицирани договори или страна по класифициран договор;

ж) **“Нарушаване на мерките за сигурност”** означава:

действие или бездействие, противоречащо на националното законодателство, водещо до или даващо възможност за нерегламентиран достъп до класифицирана информация;

з) **“Нерегламентиран достъп до класифицирана информация”** означава: разкриване, злоупотреба, изменение, увреждане, предоставяне, нерегламентирано унищожаване на класифицирана информация, както и всякакви други действия, водещи до нарушаване на мерките за защитата ѝ или до загубване на такава информация;

и) **“Разрешение за достъп”** означава:

положително решение, произтичащо от процедура по проучване, което определя лоялността и надеждността на лице в съответствие с условията, определени от националното законодателство. На базата на това положително решение на лицето може да се даде достъп до класифицирана информация с определено ниво на класификация;

й) **“Удостоверение за сигурност”** означава:

положително решение, произтичащо от процедура по проучване, което определя физическата и организационна способност на юридическо лице да защитава класифицираната информация по подходящ начин в съответствие с условията, определени от националното законодателство. На базата на това положително решение на юридическото лице може да се даде достъп до класифицирана информация с определено ниво на класификация;

к) **“Принципът необходимост да се знае”** означава:

принцип, в съответствие с който се предоставя достъп до класифицирана информация само на лице, което при изпълнение на служебните си задължения или при изпълнение на конкретно възложени задачи има необходимост от достъп до такава информация.



л) **“Компетентен орган по сигурността”** означава: органът, който в съответствие с националното законодателство на държавата на съответната Договаряща страна провежда държавната политика за защита на класифицираната информация, упражнява общ контрол в тази сфера, както и провежда изпълнението на това Споразумение. Тези органи са определени като такива в чл. 4 на това Споразумение;

м) **“Специализиран орган по сигурността”** означава: орган, която в съответствие с националното законодателство, притежава специална компетентност в областта на защита на класифицираната информация;

н) **“Трета страна”** означава: държава или международна организация, която не е страна по това Споразумение или физическо или юридическо лице, което не отговаря на съответните национални изисквания за получаване на достъп до класифицирана информация, включително и на принципа **“необходимост да се знае”**.

ЧЛЕН 3

НИВА НА КЛАСИФИКАЦИЯ ЗА СИГУРНОСТ

(1) Нивата на класификация за сигурност, приложими към информацията, обменяна в рамките на това Споразумение са:

а) за Румъния: **STRICT SECRET DE IMPORTANTĂ DEOSEBITĂ (TOP SECRET), STRICT SECRET (SECRET), SECRET (CONFIDENTIAL), SECRET DE SERVICIU (RESTRICTED);**

б) за Република България: **СТРОГО СЕКРЕТНО (TOP SECRET), СЕКРЕТНО (SECRET), ПОВЕРИТЕЛНО (CONFIDENTIAL), ЗА СЛУЖЕБНО ПОЛЗВАНЕ (RESTRICTED).**

(2) Договарящите страни определят съответствието на нивата на класификация за сигурност, както следва:



Румъния	Република България	Еквивалент на английски
STRICT SECRET DE IMPORTANTĂ DEOSEBITĂ	СТРОГО СЕКРЕТНО	TOP SECRET
STRICT SECRET	СЕКРЕТНО	SECRET
SECRET	ПОВЕРИТЕЛНО	CONFIDENTIAL
SECRET DE SERVICIU	ЗА СЛУЖЕБНО ПОЛЗВАНЕ	RESTRICTED

(3) Само Договарящата страна – източник има право да променя нивото на класификация за сигурност или да премахва нивото на класификация за сигурност на предоставената класифицирана информация. Определянето на ниво на класификация за сигурност на съвместно създадена класифицирана информация, промяната или премахването му, се извършва при общо съгласие на Договарящите страни.

ЧЛЕН 4 КОМПЕТЕНТНИ ОРГАНИ ПО СИГУРНОСТТА

(1) Компетентните органи по сигурността, отговорни за приложението и упражняването на съответния контрол по всички аспекти на Споразумението, са:

- в Румъния: Guvernul României, Oficiul Registrului Național al Informațiilor Secrete de Stat – ORNISS (Government of Romania, National Registry Office for Classified Information), București, str. Mureș nr. 4, sect. 1 ROMANIA;

- в Република България: Държавна комисия по сигурността на информацията – ДКСИ (State Commission on Information Security, Sofia, Angel Kanchev 1 Street, BULGARIA) ул. Ангел Кънчев № 1, София, БЪЛГАРИЯ.

(2) С цел постигане и поддържане на сходни стандарти за сигурност, компетентните органи по сигурността, при поискване, си предоставят информация относно стандартите за сигурност, процедурите и практиките за защита на класифицираната информация, прилагани от съответната Договаряща страна. По



взаимно съгласие между компетентните органи, всеки компетентен орган по сигурността, разрешава провеждането на инспекции от упълномощени лица на територията на съответната държава.

ЧЛЕН 5

МЕРКИ ЗА ЗАЩИТА НА КЛАСИФИЦИРАНА ИНФОРМАЦИЯ

(1) В съответствие с това Споразумение и националните си законодателства Договарящите страни прилагат съответни мерки за защита на класифицираната информация, която се обменя или създава по това Споразумение. На тази информация се осигурява същото ниво на защита, като на собствената класифицирана информация със съответно ниво на класификация за сигурност, дефинирано в член 3.

(2) Договарящата страна-получател не може да понижава или да премахва нивото на класификация за сигурност на получената информация без предварителното писмено съгласие на компетентния орган по сигурността на Договарящата страна – източник.

(3) Договарящата страна-получател се задължава:

а) да не предоставя класифицирана информация на трета страна без предварително писмено съгласие на Договарящата страна – източник;

б) да осигури ниво на класификация за сигурност на класифицираната информация, еквивалентно на нивото, дадено от Договарящата страна – източник;

в) да не използва класифицираната информация за цели, различни от тези, за които е била предоставена;

г) да гарантира частните права, като патентни, авторски права или търговски тайни, включени в класифицираната информация.

(4) Договарящата страна – източник гарантира, че Договарящата страна – получател е информирана относно:

а) грифовете за сигурност на информацията и условията за разпространяване или за ограничаване на използването ѝ,



както и че тази информация носи съответната маркировка за това;

б) за последващи промени в нивата на класификация за сигурност.

(5) Ако друго споразумение, сключено между Договарящите страни, съдържа по-ограничителни разпоредби относно обмена и защитата на класифицираната информация, прилагат се тези разпоредби.

(6) В случай на невъзможност класифицирана информация, създадена или обменена по това Споразумение, да се защитава или да бъде върната, тя се унищожават незабавно. Договарящата страна – получател уведомява компетентния орган по сигурността на Договарящата страна – източник за унищожаването при първа възможност.

ЧЛЕН 6

ПРЕНАСЯНЕ НА КЛАСИФИЦИРАНА ИНФОРМАЦИЯ

(1) Класифицирана информация се пренася чрез дипломатически или военни куриери или чрез други средства, одобрени от компетентните органи по сигурността. Получаващият компетентен орган по сигурността потвърждава получаването на класифицираната информация.

(2) В случай, че трябва да се пренесе голяма пратка, съдържаща класифицирана информация, компетентните органи по сигурността взаимно съгласуват и одобряват средствата за транспортиране, маршрута и мерките за сигурност за всеки отделен случай.

(3) Обмен на класифицирана информация чрез информационни и комуникационни системи се извършва в съответствие с процедурите за сигурност, съдържащи се в националното законодателство.



ЧЛЕН 7

ГРИФОВЕ ЗА СИГУРНОСТ

(1) Договарящата страна-получател маркира класифицираната информация на Договарящата страна-източник с еквивалентния гриф за сигурност в съответствие с чл. 3 на това Споразумение.

(2) Класифицирана информация, създадена съвместно, се маркира от Договарящата страна, на чиято територия е била създадена информацията. В този случай тази Договаряща страна ще бъде считана за Договаряща страна-източник. Договарящата страна-източник може да предоставя съвместно създадена информация на трета страна само след предварително писмено съгласие на другата Договаряща страна.

(3) Класифицирана информация, която е създадена от Договарящата страна-получател на базата на класифицирана информация или част от нея, предоставена от Договарящата страна - източник, се маркира с гриф за сигурност, който е не по-нисък от грифа за сигурност на предоставената класифицирана информация.

ЧЛЕН 8

ПРЕВОД, РАЗМНОЖАВАНЕ, УНИЩОЖАВАНЕ

(1) Преводът и размножаването на класифицирани документи, маркирани с ниво на класификация за сигурност **STRICT SECRET DE IMPORTANȚĂ DEOSEBITĂ / СТРОГО СЕКРЕТНО/ TOP SECRET** се извършва единствено след писмено разрешение на компетентния орган по сигурността на Договарящата страна -източник.

(2) Всички преводи на класифицирана информация носят грифа за сигурност на оригинала и подходяща анотация на езика, на който се преведени, в която се посочва, че преводът съдържа класифицирана информация на Договарящата страна-източник.

(3) При размножаване или копиране на класифицирана информация, грифът за сигурност на оригинала също трябва да бъде възпроизведен или отбелязан на всяко копие. Към тази размножена или копирана информация се прилагат същите мерки за защита като



за оригиналната информация. Броят на копията трябва да бъде в рамките на необходимия брой за служебни нужди.

(4) Класифицираната информация се унищожава или видоизменя по такъв начин, че да не може да бъде възстановена изцяло или отчасти.

(5) Класифицирана информация, маркирана с ниво на класификация за сигурност STRICT SECRET DE IMPORTANTĂ DEOSEBITĂ/ СТРОГО СЕКРЕТНО / TOP SECRET, не се унищожава. Такава класифицирана информация се връща на Договарящата страна - източник.

(6) Договарящата страна - източник може изрично да забрани размножаването, видоизменянето или унищожаването на класифицирана информация, чрез отбелязване върху съответния носител на класифицирана информация или чрез изпращане на последващо писмено уведомление. В този случай класифицираната информация, подлежаща на унищожаване, се връща обратно на Договарящата страна – източник, с изключение на случаите по чл. 5, ал.6.

ЧЛЕН 9 РАЗРЕШЕНИЯ ЗА ДОСТЪП/УДОСТОВЕРЕНИЯ ЗА СИГУРНОСТ

(1) Всяка Договаряща страна гарантира, че всяко лице, което в резултат на изпълнение на служебните си задължения или при изпълнение на конкретно възложени задачи, има необходимост от достъп до класифицирана информация, притежава валидно и съответно разрешение за достъп до класифицирана информация, издадено в съответствие с националното законодателство.

(2) При поискване, компетентните органи по сигурността/специализираните органи по сигурността на Договарящите страни, в съответствие с националното законодателство, си обменят информация по отношение на проучените физически или юридически лица.



(3) При поискване компетентните органи по сигурността на всяка Договаряща страна си предоставят информация за това дали на определено физическо или юридическо лице е издадено национално разрешение за достъп/удостоверение за сигурност до необходимото ниво на класификация за сигурност.

Ако физическото или юридическо лице не притежава разрешение за достъп/удостоверение за сигурност, Компетентният орган по сигурността на всяка Договаряща страна може да поиска това физическо или юридическо лице да бъде проучено.

(4) Договарящите страни взаимно си признават валидността на разрешенията за достъп и удостоверенията за сигурност, в съответствие с националното законодателство.

(5) Компетентните органи по сигурността взаимно се уведомяват за всяко отнемане или понижаване нивото на класификация, до което разрешението за достъп/удостоверението за сигурност дава достъп, на разрешения за достъп или удостоверения за сигурност, издадени на физически или юридически лица, изпълняващи дейности, които попадат под разпоредбите на това Споразумение.

ЧЛЕН 10 ИНДУСТРИАЛНА СИГУРНОСТ

(1) Класифицирани договори се сключват и изпълняват в съответствие с националното законодателство на Договарящите страни и разпоредбите на това Споразумение.

(2) В случай, че се изпълнява класифициран договор на територията на държавата на една от Договарящите страни, органите на държавата на тази Договаряща страна са задължени да упражняват контрол по отношение на изпълнението на задълженията за защита на класифицираната информация от контрагента.

(3) Преди да се предостави на контрагент от едната Договаряща страна класифицирана информация на другата Договаряща страна, Договарящата страна-получател трябва да:



а) издаде съответно удостоверение за сигурност на контрагентите при условие, че те отговарят на изискванията за това;

б) издаде съответни разрешения за достъп на всички лица, чиито служебни задължения или конкретно възложени задачи изискват достъп до класифицирана информация, при условие, че отговарят на изискванията за това;

в) гарантира, че всички лица, имащи достъп до получена класифицирана информация, са били съответно запознати с процедурите за сигурност и техните задължения по отношение на сигурността. Тези лица трябва писмено да декларират, че напълно разбират отговорностите си и правните последици, предвидени в тяхното национално законодателство в случай, че класифицираната информация бъде предоставена на неупълномощено лице, умишлено или по непредпазливост.

(4) Всеки класифициран договор включва съответен Анекс по сигурността. В този Анекс се уточнява информацията, свързана с различните аспекти на класифицирания договор, за която е необходима защита и кое съответно ниво на класификация за сигурност следва да бъде определено на тази информация, както и изискванията за сигурност, които трябва да бъдат спазени.

(5) Договори, сключени с контрагенти, съдържащи класифицирана информация с ниво на класификация SECRET DE SERVICIU/ ЗА СЛУЖЕБНО ПОЛЗВАНЕ / RESTRICTED, съдържат подходяща клауза, определяща минималните мерки, които трябва да се приложат за защитата на такава класифицирана информация.

ЧЛЕН 11 ПОСЕЩЕНИЯ

(1) Посещения в обекти, където се създава, съхранява или работи с класифицирана информация, се разрешават само от Компетентния орган по сигурността на посещаваната страна на посетители от държавата на другата Договаряща страна, ако имат необходимост от достъп до класифицирана информация.



(2) Всяка Договаряща страна уведомява своевременно другата Договаряща страна за посетителите преди планираното посещение. При спешни случаи посещенията се организират чрез специални взаимни договорености.

(3) Приемащата Договаряща страна отговаря за инструктажа на служителите на посещавания обект или учреждение относно целта на посещението и за най-високото ниво на класификация за сигурност на информацията, която може да бъде предоставена на посещаващата Договаряща страна.

(4) Исканията за посещения се подават в писмена форма до Компетентния орган по сигурността на Договарящата страна, на чиято територия се извършва посещението.

(5) Искането за посещение съдържа следната информация:

- име, дата и място на раждане, националност, номер на паспорта (личната карта) на очаквания посетител;
- длъжност и учреждение, търговско дружество или организация, чийто представител е или към чийто състав се числи посетителя;
- удостоверение за нивото на класификация за сигурност на информацията, до което посетителят има право на достъп, посочено в разрешението на посетителя;
- име и адрес на учреждениято, търговското дружество или организацията, които ще бъдат посетени;
- име и длъжност на лицето/лицата, които ще бъдат посетени, при наличие на предварителна информация;
- цел на посещението;
- дати на пристигане и отпътуване.

(6) Всяка Договаряща страна гарантира защитата на личните данни на посетителите, в съответствие с националното си законодателство.

(7) Посетителите спазват законодателството на Договарящата страна-домакин в областта на защита на класифицираната информация.



ЧЛЕН 12

НАРУШАВАНЕ НА МЕРКИТЕ ЗА СИГУРНОСТ

(1) В случай на нарушаване на мерките за сигурност, компетентният орган по сигурността, в чиято държава се е получило нарушаване на мерките за сигурност информира компетентния орган по сигурността на другата Договаряща страна възможно най-бързо, осигурява съответното разследване и предприема необходимите мерки за намаляване на последиците в съответствие с националното си законодателство. При необходимост органите на държавата на другата Договаряща страна оказват съдействие при разследването.

(2) В случаите, когато нарушаването на мерките за сигурност се извърши в трета държава, компетентният орган по сигурността на Договарящата страна, която е предоставила информацията на третата държава, трябва да предприеме, ако е възможно, действията по ал. 1.

(3) Компетентният орган по сигурността на държавата, където са нарушени мерките за сигурност, информира писмено другата Договаряща страна за резултатите от разследването по отношение на причините за това събитие, степента на вредите и мерките, предприети за тяхното ограничаване, както и за предотвратяване на повторно нарушение.

ЧЛЕН 13

РАЗРЕШАВАНЕ НА СПОРОВЕ

Всеки спор по отношение на тълкуването или прилагането на това Споразумение се разрешава чрез консултации между компетентните органи по сигурността на двете държави, без прибегване до външна юрисдикция.

ЧЛЕН 14

РАЗХОДИ

Всяка от Договарящите страни понася съответно разходите, свързани с изпълнение на задълженията ѝ по прилагане на това Споразумение.



ЧЛЕН 15 ВЗАИМНО СЪДЕЙСТВИЕ

(1) Всяка Договаряща страна и нейните държавни органи, с правомощия в областта на защита на класифицираната информация, в съответствие с националното си законодателство, съдействат на длъжностните лица от държавата на другата Договарящата страна да изпълняват задълженията си и да упражняват правата си в съответствие с разпоредбите на това Споразумение.

(2) При необходимост компетентните органи по сигурността на Договарящите страни провеждат консултации по специфични технически аспекти, засягащи приложението на това Споразумение.

(3) Компетентните органи по сигурността взаимно си предоставят информация, необходима за прилагането на разпоредбите на това Споразумение.

ЧЛЕН 16 ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

(1) Това Споразумение се сключва за неопределен срок и влиза в сила от датата на получаване на последното писмено уведомление, с което Договарящите страни се информират взаимно, че са били изпълнени всички вътрешноправни процедури за неговото влизане в сила.

(2) Това Споразумение може да бъде изменяно и допълвано по взаимно съгласие на Договарящите страни. Тези изменения или допълнения се извършват в писмена форма и влизат в сила съгласно процедурата, предвидена в ал. 1.

(3) Всяка Договаряща страна има право да прекрати действието на Споразумението писмено по всяко време. В този случай Споразумението се прекратява с изтичане на 6 (шест) месеца след датата на получаването на уведомлението за прекратяване от другата Договаряща страна.

(4) Ако действието на Споразумението бъде прекратено, цялата класифицирана информация, предоставена по Споразумението



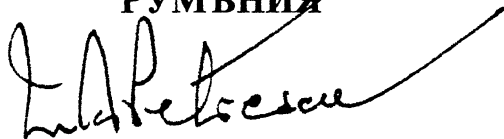
продължава да бъде защитавана съгласно горепосочените разпоредби, до момента в който Договарящата страна-източник освободи Договарящата страна-получател от това задължение.

(5) Всяка Договаряща страна незабавно уведомява другата Договаряща страна за всяко изменение в националното си законодателство, което може да окаже влияние на защитата на класифицираната информация по това Споразумение. В този случай Договарящите страни се консултират, за да обсъдят възможни изменения в това Споразумение. Междувременно класифицираната информация се защитава по гореописания начин.

(6) С влизане в сила на това Споразумение Споразумението между Правителството на Румъния и Правителството на Република България за защита на обменяната секретна военна информация, подписано в София на 29 март 2000 г. се прекратява.

Подписано в Букурещ на 13 април 2006 г., в два еднообразни екземпляра, всеки от които на румънски, български и английски език, като трите текста имат еднаква сила. В случай на различия при тълкуването, меродавен е текстът на английски език.

**ЗА ПРАВИТЕЛСТВОТО НА
РУМЪНИЯ**

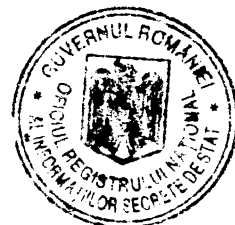


ПРОФ. Д-Р МАРИУС ПЕТРЕСКУ
Държавен секретар
Генерален директор на
Националната регистратура за
класифицирана информация

**ЗА ПРАВИТЕЛСТВОТО НА
РЕПУБЛИКА БЪЛГАРИЯ**



ЦВЕТА МАРКОВА
Председател на Държавната
комисия по сигурността на
информацията



AGREEMENT

BETWEEN

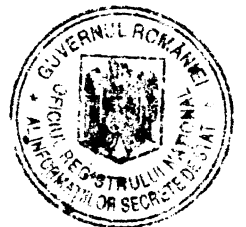
THE GOVERNMENT OF ROMANIA

AND

THE GOVERNMENT OF THE REPUBLIC OF BULGARIA

ON MUTUAL PROTECTION

OF CLASSIFIED INFORMATION



The Government of Romania and the Government of the Republic of Bulgaria, hereafter called the Contracting Parties,

Realizing that good cooperation may require exchange of classified information between the Contracting Parties,

Desiring to create a set of rules regulating the mutual protection of classified information applicable to any future co-operation agreements and classified contracts, which will be implemented between the Contracting Parties, containing or providing for access to classified information,

Have agreed on the following:

ARTICLE 1 GENERAL PROVISIONS

(1) This Agreement shall form the basis of any activity involving, in compliance with national legislation, the exchange of Classified Information between the Contracting Parties directly or through other state bodies or legal entities.

(2) The decision concerning the exchange of the Classified Information between the Contracting Parties is taken in accordance with their national legislation.

(3) The Contracting Parties shall fulfill their obligations stipulated in this Agreement, according to the terms set forth herein, on the base of equality and mutual benefit principles.

(4) This Agreement shall not affect the obligations of both Contracting Parties which stem from other international agreements and 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, regardless of its physical form, to which a security classification level has been assigned in compliance with national legislation and which shall be protected accordingly;

b) Classified Document means:

any recorded Classified Information, regardless of its physical form and characteristics, including, without limitation, the following carriers: handwritten or typed paper, seals applications used for processing data, maps, tables, photographs, pictures, pigmentation, engravings, drawings or parts thereof, sketches, rough copies, notes, carbon copies, ink ribbons or for reproducing by any means or process sounds, voices, magnetic or video or electronic or optical recordings in any form, as well as portable automatic data processing equipment with a fixed or removable data storage carrier;

c) Classified Material means:

any technical item, prototype, equipment, installation, device or weapon either manufactured or in a process of manufacture, as well as the components used for their manufacture, containing Classified Information;

d) Security Classification Marking means:

a marking stating the security classification level of Classified Information, in accordance with the national legislation of the states of the Contracting Parties;

e) Classified Contract or Sub-Contract means:

an agreement concluded, in compliance with the national legislation, between Contractors or between Contractor and Sub-Contractor which contains and/or provides for access to Classified Information in the process of its execution;

f) Contractor or Sub-Contractor means:

an individual or a legal entity possessing the legal capability to conclude Classified Contracts or is a party to a Classified Contract;



g) Breach of Security means:

an act or omission contrary to national legislation, which results or may result in an Unauthorised Access to Classified Information;

h) Unauthorised Access to Classified Information means:

disclosure, misuse, change in, damage, submission, unauthorised destruction of Classified Information, as well as any other acts, resulting in breach of protective measures or loss of such information;

i) Personnel Security Clearance means:

a positive decision stemming from a vetting procedure which is to determine the loyalty and trustworthiness of a person and affirm the conformity with the conditions set out in national legislation. On the basis of this positive decision access to information of a certain level of classification may be granted to such a person;

j) Facility Security Clearance means:

a positive decision stemming from a vetting procedure which is to determine the physical and organisational capability of a legal entity to protect Classified Information appropriately and affirm the conformity with the conditions set out in national regulations. On the basis of this positive decision access to information of a certain level of classification may be granted to such an entity;

k) "Need to Know" principle means:

a principle according to which access to Classified Information may only be granted to a person who, in carrying out his official duties or tasks, needs access to such information;

l) Competent Security Authority means:

the authority which in compliance with the national legislation of the state of the respective Contracting Party performs the state policy for the protection of Classified Information, exercises overall control in this sphere as well as conducts the implementation of this Agreement, and is determined as such in Article 4 of this Agreement;

m) Specialised Security Authority means:

the institution which, in compliance with the national legislation has specific competences in the field of the protection of the Classified Information;



n) **Third Party** means:

a state or an international organisation, which is not a party to this Agreement or an individual or a legal entity which does not respond to the respective national requirements of access to Classified Information, including the “need to know” principle.

ARTICLE 3 SECURITY CLASSIFICATION LEVELS

(1) The security classification levels applicable to information exchanged within the framework of this Agreement are:

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

b) for the Republic of Bulgaria: СТРОГО СЕКРЕТНО (TOP SECRET), СЕКРЕТНО (SECRET), ПОВЕРИТЕЛНО (CONFIDENTIAL) and ЗА СЛУЖЕБНО ПОЛЗВАНЕ (RESTRICTED).

(2) The Contracting Parties have determined that the equivalence of the security classification levels is as follows:

Romania	Republic of Bulgaria	English Equivalent
STRICT SECRET DE IMPORTANTĂ DEOSEBITĂ	СТРОГО СЕКРЕТНО	TOP SECRET
STRICT SECRET	СЕКРЕТНО	SECRET
SECRET	ПОВЕРИТЕЛНО	CONFIDENTIAL
SECRET DE SERVICIU	ЗА СЛУЖЕБНО ПОЛЗВАНЕ	RESTRICTED

(3) Only the originating Contracting Party is authorised to change the security classification level or to declassify the transmitted Classified Information. The assignment of security classification level to jointly created



Classified Information, its change or the declassification of this information shall be made upon common consent of the Contracting Parties.

ARTICLE 4 COMPETENT SECURITY AUTHORITIES

(1) The Competent Security Authorities responsible for the implementation and the relevant control of all aspects of this Agreement are:

- **In Romania:** Guvernul României, Oficiul Registrului Național al Informațiilor Secrete de Stat – ORNISS București, str. Mureș nr. 4, sect. 1, ROMÂNIA (Government of Romania, National Registry Office for Classified Information, Bucharest, 4 Mureș Street, Sector 1, ROMANIA);

- **In the Republic of Bulgaria:** Държавна Комисия по Сигурността на Информацията-ДКСИ, София, ул. Ангел Кънчев No 1, БЪЛГАРИЯ, (State Commission on Information Security, Sofia, Angel Kanchev 1 Street, BULGARIA).

(2) In order to achieve and maintain comparable standards of security, the Competent Security Authorities shall, on request, provide each other with information about the security standards, procedures and practices for protection of Classified Information applied by the respective Contracting Party. Each Competent Security Authority shall, by mutual consent, enable inspection visits of authorised officials in both countries.

ARTICLE 5 CLASSIFIED INFORMATION PROTECTION MEASURES

(1) In compliance with this Agreement and their national legislations, the Contracting Parties shall implement all appropriate measures for protection of Classified Information which is exchanged or created under this Agreement. The same level of protection shall be ensured for such Classified Information as it is provided for the national Classified Information, with the corresponding security classification level pursuant to Article 3.

(2) The receiving Contracting Party shall neither use a lower security classification level for the received Classified Information nor declassify this



information without the prior written consent of the Competent Security Authority of the originating Contracting Party.

(3) The receiving Contracting Party is obliged:

a) not to disclose Classified Information to a Third Party without a prior written consent of the originating Contracting Party;

b) to afford Classified Information a security classification level equivalent to that provided by the originating Contracting Party;

c) not to use Classified Information for purposes other than those it has been provided for;

d) to guarantee the private rights such as patent rights, copyrights or trade secrets that are involved in Classified Information.

(4) The originating Contracting Party shall ensure that the receiving Contracting Party is informed of:

a) Security Classification Markings of information and any conditions of release or limitation on its use, and that information is so marked;

b) any subsequent change in security classification levels.

(5) If any other Agreement concluded between the Contracting Parties contains stricter regulations regarding the exchange or protection of Classified Information, these regulations shall apply.

(6) In case it is impossible to protect and return Classified Information created or exchanged according to this Agreement, the Classified Information shall be destroyed immediately. The receiving Contracting Party shall notify the Competent Security Authority of the originating Contracting Party about such a destruction of the Classified Information as soon as possible.



ARTICLE 6 TRANSMISSION OF CLASSIFIED INFORMATION

(1) Classified Information shall be transmitted by diplomatic or military couriers or other means approved by the Competent Security Authorities. The receiving Competent Security Authority shall acknowledge receipt of the Classified Information.

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

(3) The exchange of Classified Information through information and communications systems shall take place in accordance with the security procedures set out in national legislation.

ARTICLE 7 SECURITY CLASSIFICATION MARKINGS

(1) The receiving Contracting Party shall mark the Classified Information of the originating Contracting Party with equivalent Security Classification Marking in accordance with Article 3 of this Agreement.

(2) Classified Information created jointly shall be marked by the Contracting Party within the territory of which this information has been created. In this case, this Contracting Party shall be considered originating Contracting Party. The originating Contracting Party may transmit the jointly created Classified Information to a Third Party only upon prior written consent of the other Contracting Party.

(3) Classified Information created by the receiving Contracting Party on the basis of Classified Information or part of it transmitted by the originating Contracting Party shall be marked with a Security Classification Marking which is not lower than the Security Classification Marking of the transmitted Classified Information.



ARTICLE 8 TRANSLATION, REPRODUCTION, DESTRUCTION

(1) Classified Documents marked with a security classification level STRICT SECRET DE IMPORTANTĂ DEOSEBITĂ / ЦТРОГО СЕКРЕТНО / TOP SECRET shall be translated or copied only by written permission of the Competent Security Authority of the originating Contracting Party.

(2) Any translation of Classified Information shall bear the Security Classification Marking of the original and a suitable annotation in the language of translation indicating that the translated material contains Classified Information of the originating Contracting Party.

(3) When Classified Information is reproduced or copied, all original Security Classification Markings thereon shall also be reproduced or marked on each copy. Such reproduced or copied information shall be placed under the same protective measures as the original information. The number of copies shall be limited to that required for official purposes.

(4) Classified Information shall be destroyed or modified insofar as to forestall its reconstruction in whole or in part.

(5) Classified Information of the security classification level STRICT SECRET DE IMPORTANTĂ DEOSEBITĂ/ ЦТРОГО СЕКРЕТНО / TOP SECRET shall not be destroyed. It shall be returned to the originating Contracting Party.

(6) The originating Contracting Party may expressly prohibit reproduction, alteration or destruction of a Classified Information by marking the relevant carrier of Classified Information or sending subsequent written notice. In such case, the Classified Information subject to destruction shall be returned to the originating Contracting Party, except in the case referred to in Article 5, paragraph 6.



ARTICLE 9 SECURITY CLEARANCES

(1) Each Contracting Party shall guarantee that any individual, who, due to his official duties or tasks, needs access to Classified Information, holds a valid and appropriate Personnel Security Clearance, issued in accordance with the national legislation.

(2) Upon request, the Competent Security Authorities/ Specialised Security Authorities of the Contracting Parties, in compliance with national legislation, shall exchange information related to the vetted individuals or legal entities.

(3) Upon request, the Competent Security Authority of each Contracting Party shall provide information whether an individual or a legal entity has been issued a national Personnel Security Clearance/ Facility Security Clearance corresponding to the required security classification level.

If an individual or a legal entity does not hold a Personnel Security Clearance/ Facility Security Clearance the Competent Security Authority of each Contracting Party may request for that individual or legal entity to be security cleared.

(4) The Contracting Parties shall mutually recognize the validity of Personnel Security Clearances and Facility Security Clearances, in accordance with national legislation.

(5) The Competent Security Authorities shall notify each other on any withdrawal or downgrading of Personnel Security Clearances or Facility Security Clearances, issued to individuals or legal entities which perform activities under the provisions of this Agreement.

ARTICLE 10 INDUSTRIAL SECURITY

(1) Classified Contracts shall be concluded and implemented in accordance with the national legislation of the Contracting Parties and the provisions of this Agreement.



(2) In case a Classified Contract is performed within the territory of the state of one of the Contracting Parties, the authorities of the state of that Contracting Party are obliged to exercise control regarding the fulfillment of the Classified Information protection obligations by the Contractor.

(3) Prior to releasing to Contractors from the state of either Contracting Party any Classified Information of the other Contracting Party, the receiving Contracting Party shall:

a) grant an appropriate Facility Security Clearance to the Contractors on condition they have fulfilled the requirements for its issue;

b) grant an appropriate Personnel Security Clearance to all individuals whose official duties or tasks require access to Classified Information on condition they have fulfilled the requirements for its issue;

c) ensure that all individuals having access to received Classified Information have been appropriately briefed on security procedures and their security obligations. All such individuals shall acknowledge in writing that they fully understand their responsibilities and the consequences which the national legislation provides when Classified Information passes to unauthorised individuals either by intent or negligence.

(4) Every Classified Contract shall include an appropriate security annex. The Security annex shall specify the information connected with various aspects of the Classified Contract which require protection and the corresponding security classification level that is to be assigned thereto, as well as the security requirements that are to be met.

(5) Classified Contracts placed with contractors involving Classified Information at SECRET DE SERVICIU / 3A СЛЮЖЕБНО ПОЛІЗБАHE / RESTRICTED level shall contain an appropriate clause identifying the minimum measures to be implemented for the protection of such Classified Information.



ARTICLE 11 VISITS

(1) Visits to premises where Classified Information is created, handled or stored, shall be allowed only by the Competent Security Authority of the visited state to visitors from the state of the other Contracting Party, if they need access to Classified Information.

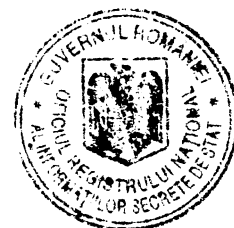
(2) Each Contracting Party shall notify in due time the other Contracting Party of expected visitors prior to the planned visit. Short notice visits can be arranged in urgent cases by special mutually determined arrangements.

(3) The host Contracting Party shall be responsible for briefing specifically the personnel of the facilities and establishments that are to be visited on the decisions referring to the objective of the visit and the highest level of Classified Information that is to be released to the visiting Contracting Party.

(4) Request concerning carrying out the visit shall be forwarded in written form to the Competent Security Authority of the Contracting Party whose territory shall be visited.

(5) The request for visit shall contain the following information:

- name of the proposed visitor, date and place of birth, nationality and passport (ID card) number;
- official status of the visitor together with the name of the establishment, company or organization which he/she represents or to which he/she belongs;
- certification of level of security clearance of the visitor;
- name and address of the establishment, company or organization to be visited;
- name and status of the person(s) to be visited, if known;
- purpose of the visit;



- dates of arrival and departure.

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

(7) All visitors shall comply with the legislation on protection of Classified Information of the host Contracting Party's state.

ARTICLE 12 BREACH OF SECURITY

(1) In case of a Breach of Security, the Competent Security Authority of the state where the Breach of Security occurred shall inform promptly the Competent Security Authority of the other Contracting Party, shall ensure proper investigation of such event and shall take the necessary measures to reduce the prejudices, in accordance with national legislation. The authorities of the state of the other Contracting Party shall, if required, cooperate in the investigation.

(2) In case the Breach of Security occurs in a third country, the Competent Security Authority of the Contracting Party which transmitted the information to the third country shall take if possible the actions as of paragraph 1.

(3) The Competent Security Authority of the state where the Breach of Security occurred shall inform in writing the other Contracting Party of the results of the investigation regarding the causes of the event, the extent of the damage and the measures taken for its limitation and for the prevention of its recurrence.

ARTICLE 13 SETTLEMENT OF DISPUTES

Any dispute regarding the interpretation or implementation of this Agreement shall be settled by consultation between the Competent Security Authorities of the two states, without recourse to outside jurisdiction.



**ARTICLE 14
EXPENSES**

Each Contracting Party shall cover its own expenses in the course of the implementation of this Agreement.

**ARTICLE 15
MUTUAL ASSISTANCE**

(1) Each Contracting Party and the authorities of its state with responsibilities in the field of protection of Classified Information, in compliance with the national legislation, shall assist the personnel from the state of the other Contracting Party in fulfilling the obligations and exercising the rights in accordance with the provisions of this Agreement.

(2) Should the need arise the Competent Security Authorities of the Contracting Parties shall consult each other on specific technical aspects concerning the implementation of this Agreement.

(3) The Competent Security Authorities shall mutually provide information required to the implementation of the provisions of this Agreement.

**ARTICLE 16
FINAL PROVISIONS**

(1) This Agreement is concluded for an indefinite period of time and enters into force on the date of 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) This Agreement may be amended and supplemented on the basis of the mutual consent of both Contracting Parties. Such amendments or supplements shall be made in writing and shall enter into force in accordance with the provisions of paragraph 1 of this Article.

(3) Each Contracting Party has the right to terminate this Agreement in writing at any time. In such case the validity of the Agreement will expire



after 6 (six) months following the day on which the termination notice has been received by the other Contracting Party.

(4) Should the validity of this Agreement expire, all Classified Information provided pursuant to this Agreement shall continue to be protected in accordance with the provisions set forth herein, until the originating Contracting Party dispenses the receiving Contracting Party from this obligation.

(5) Each Contracting Party shall promptly notify the other Contracting Party of any changes to its national legislation that would affect the protection of Classified Information under this Agreement. In such case, the Contracting Parties shall consult to consider possible changes to this Agreement. In the meantime, Classified Information shall continue to be protected as described herein.

(6) When this Agreement enters into force, the Agreement between the Government of Romania and the Government of the Republic of Bulgaria on the protection of exchanged classified military information, signed at Sofia, on 29th March, 2000 shall be terminated.

Done in Bucharest, on 13th April 2006, in two original copies, each one in the Romanian, Bulgarian and English languages, all texts having equal validity. In case of differences in 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 REPUBLIC OF
BULGARIA**



TSVETA MARKOVA
Chairperson
of the State Commission on
Information Security

*Conform cu
originea*



