

**ACORD DE SECURITATE**

**ÎNTRE**

**ROMÂNIA**

**ȘI**

**REPUBLICA PORTUGHEZĂ**

**PRIVIND PROTECȚIA RECIPROCĂ A INFORMAȚIILOR CLASIFICATE**

România și Republica Portugheză,

Denumite în continuare Părți,

În scopul asigurării protecției informațiilor clasificate schimbate între Părți prin intermediul unor instituții publice sau persoane juridice de drept public sau privat care gestionează informații clasificate ale celeilalte Părți;

Dorind să creeze un ansamblu de reglementări privind protecția reciprocă a informațiilor clasificate schimbate între Părți,

Au convenit următoarele:

## ARTICOLUL 1 OBIECTUL

Prezentul Acord de Securitate, denumit în continuare Acord, stabilește reglementările de securitate care vor sta la baza tuturor acordurilor sau contractelor privind schimbul de informații clasificate, încheiate sau care urmează să fie încheiate între instituțiile publice sau alte persoane juridice de drept public sau privat ale Părților, autorizate corespunzător în acest sens.

## ARTICOLUL 2 DOMENIUL DE APLICARE

1. Prezentul Acord va sta la baza tuturor activităților ce implică schimbul de informații clasificate între Părți referitor la:
  - a. cooperarea între Părți în domeniul apărării naționale și în orice alte aspecte legate de securitatea națională;
  - b. cooperarea, proiectele comune, contractele sau oricare alte raporturi între organismele de stat sau alte persoane juridice de drept public sau privat ale Părților în domeniul apărării naționale și orice alte aspecte privind securitatea națională;
  - c. vânzarea de echipamente, produse și know-how.
2. Prezentul Acord nu va fi invocat de nici una dintre Părți pentru a obține informațiile clasificate pe care cealaltă Parte le-a primit de la un terț.

### ARTICOLUL 3 DEFINIȚII

În sensul prezentului Acord:

**a. informație clasificată înseamnă:**

orice informație, document sau material, indiferent de forma sa fizică, căreia i s-a atribuit o anumită clasificare de securitate în conformitate cu legislația în vigoare și care va fi protejată corespunzător;

**b. document clasificat înseamnă:**

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

**c. material clasificat înseamnă:**

orice obiect sau parte a unui mecanism, prototip, echipament, armă sau altele asemenea, fabricat mecanic sau manual, ori aflat în curs de fabricație și căruia i s-a atribuit o clasificare de securitate;

**d. clasificare de securitate înseamnă:**

atribuirea unei clase sau nivel de clasificare în conformitate cu legislațiile în vigoare ale Părților;

**e. contract clasificat înseamnă:**

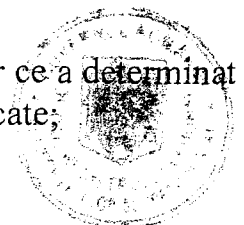
un acord între doi sau mai mulți contractanți prin care se stabilesc și se definesc drepturile și obligațiile acestora și care conține sau implică acces la informații clasificate;

**f. contractant sau sub-contractant înseamnă:**

o persoană fizică sau juridică ce are capacitatea legală de a încheia contracte clasificate;

**g. incident de securitate înseamnă:**

o acțiune sau inacțiune contrară legislațiilor în vigoare ale Părților ce a determinat sau este de natură să determine compromiterea informației clasificate;



- i. **compromiterea informației clasificate** înseamnă:  
acea situație când, datorită unui Incident de Securitate sau a unei activități ostile, informațiile clasificate și-au pierdut confidențialitatea, integritatea sau disponibilitatea sau când serviciile și resursele ajutoare și-au pierdut integritatea sau disponibilitatea. Aceasta include pierderea, divulgarea, parțială sau totală, modificarea ori distrugerea neautorizată sau repudierea serviciului;
- l. **anexa de securitate** înseamnă:  
un document emis de către autoritatea îndreptățită ca parte a oricărui contract sau sub-contract clasificat, ce identifică cerințele de securitate sau acele elemente ale contractului care necesită protecție;
- j. **lista clasificărilor de securitate** înseamnă:  
evidența informațiilor clasificate, materialelor și activităților aferente unui contract clasificat și clasificările de securitate ale acestora, inclusă în anexa de securitate;
- k. **certificatul de securitate a personalului** înseamnă:  
documentul care atestă faptul că posesorul acestuia poate avea acces la informații clasificate cu o anumită clasificare de securitate, potrivit principiului necesității de a cunoaște;
- l. **certificatul de securitate industrială** înseamnă:  
documentul prin care se atestă că o persoană juridică este abilitată să deruleze activități industriale care presupun accesul la informații clasificate cu o anumită clasificare de securitate;
- m. **necesitatea de a cunoaște** înseamnă:  
principiul conform căruia accesul la informații clasificate se acordă în mod individual numai persoanelor care, pentru îndeplinirea îndatoririlor de serviciu, trebuie să lucreze cu astfel de informații sau să aibă acces la acestea;
- n. **Autoritatea Competentă de Securitate** înseamnă:  
instituția investită cu autoritate la nivel național care, conform legislației în vigoare, asigură implementarea unitară a măsurilor de protecție a informațiilor clasificate;
- o. **Autoritate Desemnată de Securitate** înseamnă:  
instituția care, în conformitate cu legislația în vigoare a Părților coordonată de Autoritatea Competentă de Securitate în domeniul protecției informațiilor clasificate este abilitată să stabilească propriile structuri și măsuri pentru domeniul său de activitate și conform competențelor specifice;
- p. **Partea Emitentă** înseamnă:



Partea care transmite informațiile clasificate celeilalte Părți;

**Partea Primitoare** înseamnă:

Partea care primește informațiile clasificate transmise acesteia de către Partea Emitentă;

**Tert** înseamnă:

orice organizație internațională sau stat care nu este Parte la prezentul Acord.

#### ARTICOLUL 4 AUTORITĂȚILE COMPETENTE DE SECURITATE

1. Autoritățile Competente de Securitate responsabile, la nivel național, de implementarea și controlul măsurilor prevăzute în prezentul Acord sunt:

<p>Pentru România:</p> <p>Guvernul României</p> <p>Oficiul Registrului Național al Informațiilor Secrete de Stat (ORNISS)</p> <p>București – Str. Mureș nr. 4, Sector 1</p> <p>ROMÂNIA</p>	<p>Pentru Republica Portugheză:</p> <p>Autoridade Nacional de Segurança</p> <p>Presidência do Conselho de Ministros</p> <p>Rua da Junqueira, 69</p> <p>1300-342 Lisboa</p> <p>PORTUGAL</p>
--	--

2. Pentru a menține aceleași standarde de securitate, fiecare Autoritate Competentă de Securitate va furniza, la cerere, celeilalte Autorități Competente de Securitate informații referitoare la organizarea, procedurile sale de securitate cât și despre legislația în vigoare referitoare la protecția informațiilor clasificate.
3. În vederea asigurării unei strânse cooperări privind implementarea prezentului Acord, Autoritățile Competente de Securitate își pot acorda asistență și se pot consulta reciproc la solicitarea uneia dintre Părți.



## ARTICOLUL 5 ECHIVALENȚA CLASIFICĂRILOR DE SECURITATE

Părțile Contractante au stabilit următoarea echivalență a clasificărilor naționale de securitate:

România	Republica Portugheză	Echivalentul în limba engleză
STRICT SECRET DE IMPORTANTĂ DEOSEBITĂ	MUITO SECRETO	TOP SECRET
STRICT SECRET	SECRETO	SECRET
SECRET	CONFIDENCIAL	CONFIDENTIAL
SECRET DE SERVICIU	RESERVADO	RESTRICTED

## ARTICOLUL 6 PROTECȚIA INFORMAȚIILOR CLASIFICATE

1. Protecția și utilizarea informațiilor clasificate schimbate între Părți sunt guvernate de următoarele reguli:
  - a. Partea Primitoare va asigura tuturor informațiilor clasificate schimbate, primite, produse sau elaborate același grad de protecție prevăzut pentru propriile informații clasificate cu o clasificare de securitate echivalentă;
  - b. accesul la informații clasificate este permis, cu respectarea principiului necesității de a cunoaște, numai persoanelor care, în îndeplinirea funcțiilor, necesită acces la Informații clasificate și dețin certificat de securitate a Personalului valabil pentru acces la informațiile clasificate SECRET / CONFIDENCIAL / CONFIDENTIAL sau de nivel superior;
  - c. reprezentanții unei Părți au acces la informațiile clasificate SECRET DE SERVICIU / RESERVADO / RESTRICTED ale celeilalte Părți cu respectarea principiului necesității de a cunoaște, dacă îndeplinesc cerințele privind accesul la astfel de informații clasificate în conformitate cu legislația națională a Părții pe care o reprezintă.



2. Partea Primitoare va marca informațiile clasificate primite cu propriul său echivalent al marcajului de clasificare de securitate conform echivalențelor stabilite în articolul 5 al prezentului Acord.
3. Partea Emitentă va informa Partea Primitoare asupra oricăror modificări survenite în clasificarea de securitate a informațiilor clasificate transmise.
4. Partea Primitoare nu va utiliza un nivel mai scăzut de clasificare și nici nu va declassifica informațiile clasificate primite, fără acordul prealabil scris al Părții Emitente.
5. Traducerile și multiplicările informațiilor clasificate se vor face conform următoarelor proceduri:
  - a) persoanele vor deține certificate de securitate a personalului corespunzătoare;
  - b) traduceri și multiplicări vor fi marcate cu același nivel de clasificare și vor fi protejate în același mod ca și informațiile clasificate originale;
  - c) traduceri și numărul de copii se vor limita la numărul de exemplare necesare scopurilor oficiale;
  - d) traduceri vor fi însoțite de o notă în limba în care s-a efectuat traducerea în care se va menționa că documentul conține informații clasificate primite de la Partea Emitentă.
6. Informațiile clasificate marcate STRICT SECRET DE IMPORTANȚĂ DEOSEBITĂ / MUITO SECRETO / TOP SECRET vor fi traduse sau multiplicare numai cu acordul scris al Autorității Competente de Securitate a Părții Emitente în conformitate cu legislația sa în vigoare.
7. Informațiile clasificate marcate STRICT SECRET DE IMPORTANȚĂ DEOSEBITĂ / MUITO SECRETO / TOP SECRET nu vor fi distruse, ci vor fi returnate Partii Emitente.
8. Distrugerea informațiilor clasificate marcate STRICT SECRET / SECRETO / SECRET și SECRET / CONFIDENCIAL / CONFIDENCIAL se va face după obținerea acordului prealabil scris al Părții Emitente.
9. În cazul unei situații care face imposibilă protejarea și returnarea informațiilor clasificate generate sau transmise în conformitate cu prezentul Acord, informațiile clasificate vor fi distruse imediat. Partea Primitoare va informa cât mai repede posibil Partea Emitentă despre distrugerea informațiilor clasificate.



## ARTICOLUL 7 TRANSMITEREA INFORMAȚIILOR CLASIFICATE

Informațiile clasificate se transmit pe canale diplomatice, prin curier militar sau prin alte mijloace aprobate de Autoritățile Competente de Securitate.

Dacă există un volum mare de informații clasificate ce trebuie transmis, Autoritățile Competente de Securitate vor conveni pentru fiecare caz în parte asupra modalităților de transport, rutei și măsurilor de securitate.

Schimbul de informații clasificate prin intermediul sistemelor informatice și de comunicații protejate se realizează conform procedurilor de securitate stabilite de comun acord de către Autoritățile Competente de Securitate ale Părților.

Partea Primitoare va confirma în scris primirea informațiilor clasificate.

## ARTICOLUL 8 DISEMINAREA INFORMAȚIILOR

Diseminarea informațiilor clasificate către terți sau către orice persoană juridică publică sau privată de naționalitatea unui stat terț poate avea loc după obținerea acordului scris al Autorității Competente de Securitate a Părții Emitente, care poate impune noi limitări asupra diseminării.

Fiecare Parte se va asigura că informațiile clasificate primite de la cealaltă Parte sunt folosite doar în scopul pentru care au fost transmise.

## ARTICOLUL 9 PROCEDURILE DE VERIFICARE DE SECURITATE

Partile vor recunoaște reciproc certificatele de securitate a personalului și certificatele de securitate industrială emise în conformitate cu legislația în vigoare la celelalte Părți.

Autoritățile Competente de Securitate se vor informa reciproc asupra oricăror modificări privind certificatele de securitate a personalului și certificatele de securitate industrială.





La cerere, Autoritățile Competente de Securitate ale Părților, ținând seama de legislația lor în vigoare, își vor acorda asistență reciprocă la procedurile de vetting a cetățenilor săi care locuiesc pe teritoriul celeilalte Părți și a obiectivelor localizate pe teritoriul celeilalte Părți, anterioare emiterii certificatului de securitate a personalului și a certificatului de securitate industrială.

## ARTICOLUL 10 CONTRACTELE CLASIFICATE

În cazul unor contracte clasificate ce urmează a fi încheiate și derulate pe teritoriul uneia dintre Părți, Autoritatea Competentă de Securitate a celeilalte Părți va obține confirmarea prealabilă scrisă care să ateste deținerea de către contractantul propus a unui certificat de securitate industrială de nivel corespunzător.

Contractantul se angajează:

să garanteze faptul că în locațiile sale există condiții adecvate pentru procesarea informațiilor clasificate;

să dețină certificat de securitate industrială corespunzător pentru locațiile respective;

să dețină certificat de securitate a personalului pentru persoanele care derulează activități ce necesită acces la informații clasificate;

să garanteze că toate persoanele care au acces la informații clasificate sunt informate despre responsabilitățile privind protecția informațiilor clasificate, în conformitate cu legislația în vigoare;

să permită inspecții de securitate în locațiile sale efectuate de reprezentanți ai Autorităților Competente de Securitate.

Fiecare sub-contractant trebuie să îndeplinească aceleași cerințe de securitate ca și Contractantul.

Autoritatea Competentă de Securitate răspunde de urmărirea și controlul respectării de către contractant a angajamentelor prevăzute în alin.2.

Fiecare contract clasificat încheiat între Contractanții Părților, cu respectarea prevederilor prezentului Acord, va cuprinde o Anexă de Securitate corespunzătoare în care se vor regăsi cel puțin următoarele aspecte:

- a. o listă a clasificărilor de securitate;
  - b. procedura de comunicare a modificărilor survenite în clasificarea de securitate;
  - c. canalele de comunicare și mijloacele de transmisie electromagnetică;
  - d. procedura de transport a informațiilor clasificate;
  - e. autoritățile competente pentru coordonarea protecției informațiilor clasificate aferente contractului;
  - f. obligația de a notifica orice compromitere reală sau posibilă a informațiilor clasificate.
6. O copie a anexei de securitate a oricărui contract clasificat va fi înaintată Autorității Competente de Securitate a Părții din statul în care se va derula contractul clasificat pentru a permite supravegherea și controlul de securitate corespunzător.
7. Autoritățile Competente de Securitate pot conveni asupra vizitelor reciproce efectuate în scopul analizării eficienței măsurilor adoptate de contractant pentru protecția informațiilor clasificate cuprinse în contractul clasificat. vizita va fi anunțată în scris înainte cu cel puțin douăzeci de zile lucrătoare.

## ARTICOLUL 11 VIZITELE

1. Vizitele ce presupun accesul la informații clasificate efectuate de cetățenii unei Părți pe teritoriul celeilalte Părți vor fi autorizate în scris, în prealabil, de către Autoritățile Competente de Securitate sau Autoritățile Desemnate de Securitate, în conformitate cu legislația în vigoare.
2. Cererea de vizită va fi înaintată prin Autoritatea Competentă de Securitate a Părții din statul gazdă.
3. Partea gazdă va permite vizite ce presupun accesul la informații clasificate vizitatorilor din statul celeilalte Părți numai dacă aceștia :
  1. dețin certificatul de securitate a personalului de nivel corespunzător; și
  2. au fost autorizați să primească și să aibă acces la informații clasificate cu respectarea principiului necesității de a cunoaște, în conformitate cu legislația în vigoare.
4. Autoritatea Competentă de Securitate a Părții care solicită efectuarea vizitei va informa Autoritatea Competentă de Securitate a Părții gazdă despre vizita planificată printr-o cerere de vizită care trebuie primită înainte cu cel puțin douăzeci de zile lucrătoare.

5. În cazuri urgente, cererea de vizită va fi transmisă înainte cu cel puțin cinci zile lucrătoare.
6. Autoritatea Competentă de Securitate a Părții care primește cererea de vizită va informa în timp util Autoritatea Competentă de Securitate a Părții solicitante despre decizia luată.
7. Vizitele persoanelor aparținând unui terț ce presupun acces la informațiile clasificate ale Părții Emitente vor fi autorizate doar cu acordul scris al Autorității Competente de Securitate sau al Autorității Desemnate de Securitate în conformitate cu legislația în vigoare.
8. După aprobarea vizitei, Autoritatea Competentă de Securitate sau Autoritatea Desemnată de Securitate a Părții gazdă va transmite o copie a cererii de vizită funcționarului de securitate al instituției, obiectivului sau organizației ce urmează a fi vizitată.
9. Valabilitatea autorizației de vizită nu va depăși douăsprezece luni.
10. Pentru fiecare contract clasificat, Părțile pot conveni să stabilească liste cu persoanele autorizate să efectueze vizite periodice. Aceste liste sunt valabile pentru o perioadă inițială de douăsprezece luni.
11. După ce listele au fost aprobate de către Părți, detaliile ulterioare privind vizitele se vor stabili direct între reprezentanții organizațiilor implicate, în conformitate cu termenii și condițiile convenite.
12. Cererea de vizită va cuprinde:
  - a. numele și prenumele vizitatorului, locul și data nașterii, naționalitatea, numărul pasaportului sau al cărții de identitate;
  - b. numele instituției, obiectivului sau organizației de care aparține sau al cărei reprezentant este vizitatorul;
  - c. numele și adresa instituției, obiectivului sau organizației care urmează să fie vizitată;
  - d. confirmarea faptului că vizitatorul deține certificat de securitate a personalului precum și perioada de valabilitate al acestuia;
  - e. obiectul și scopul vizitei/vizitelor;



data și durata aproximativă a vizitei sau vizitelor solicitate, iar în cazul vizitelor periodice se va menționa perioada totală a vizitelor;

numele și numărul de telefon al persoanei de contact din cadrul instituției, obiectivului sau organizației ce urmează să fie vizitată, contacte anterioare și orice alte informații utile pentru a justifica vizita / vizitele;

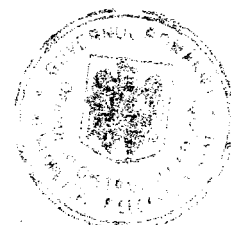
data, semnătura și ștampila oficială a Autorității Competente de Securitate sau a Autorității Desemnate de Securitate corespunzătoare.

## ARTICOLUL 12 INCIDENTE DE SECURITATE

1. În cazul producerii unor incidente de securitate privind informațiile clasificate emise sau primite de la cealaltă Parte, Autoritatea Competentă de Securitate a Părții unde a avut loc incidentul de securitate va informa de îndată Autoritatea Competentă de Securitate a celeilalte Părți și va efectua o investigație corespunzătoare.
2. În cazul în care incidentul de securitate a avut loc pe teritoriul unui stat terț, Autoritatea Competentă de Securitate a Părții transmițătoare va întreprinde acțiunile prevăzute în alin.1.
3. Dacă este necesar, cealaltă Parte va coopera la investigație.
4. În oricare dintre cazuri cealaltă Parte va fi informată în scris asupra rezultatelor și concluziilor investigației, inclusiv a motivelor pentru care s-a produs incidentul de securitate, amploarea prejudiciului și măsurile corespunzătoare întreprinse pentru limitarea acestuia.

## ARTICOLUL 13 COSTURI

Fiecare Parte va suporta propriile costuri legate de aplicarea și urmărirea îndeplinirii tuturor aspectelor din prezentul Acord.



## ARTICOLUL 14 SOLUȚIONAREA DIFERENDELOR

Orice diferend privind interpretarea sau aplicarea prezentului Acord, dacă nu va fi soluționat prin consultări între Autoritățile Competente de Securitate, se va soluționa prin negocieri pe canale diplomatice.

## ARTICOLUL 15 INTRAREA ÎN VIGOARE

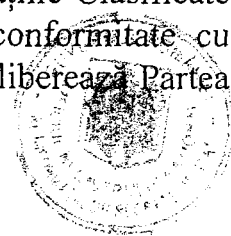
Prezentul Acord va intra în vigoare în a treizecea zi după primirea ultimei notificări în scris și prin canale diplomatice, care va statua faptul că au fost îndeplinite toate procedurile legale interne ale ambelor Părți.

## ARTICOLUL 16 AMENDAMENTE

1. Părțile pot modifica prezentul Acord pe baza unui acord reciproc scris.
2. Modificările vor intra în vigoare în conformitate cu prevederile articolului 15 al prezentului Acord.

## ARTICOLUL 17 DURATA ȘI DENUNȚAREA

1. Prezentul Acord va rămâne în vigoare pe o perioadă nedeterminată de timp.
2. Oricare dintre Părți poate denunța în orice moment prezentul Acord.
3. Denunțarea va fi notificată în scris și prin canale diplomatice și va deveni efectivă la șase luni de la data primirii respectivei notificări.
4. Până la finele cont de denunțarea prezentului Acord, toate Informațiile Clasificate furnizate în baza acestuia vor continua să fie protejate în conformitate cu prevederile stabilite în acest Acord până când Partea Emitentă eliberează Partea Primitoare de această obligație.



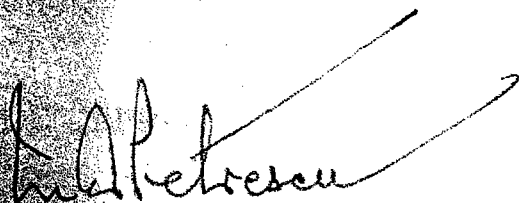


## ARTICOLUL 18 ÎNREGISTRAREA

După intrarea în vigoare a prezentului Acord, Partea pe teritoriul căreia a fost semnat îl va transmite spre înregistrare la Secretariatul Națiunilor Unite în conformitate cu art. 102 al Cartei Națiunilor Unite, și va informa cealaltă Parte despre încheierea acestei proceduri, menționând numărul înregistrării.

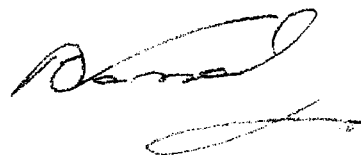
Semnat la București, la 14 mai 2008, în două exemplare originale, fiecare în limbile română, portugheză și engleză, toate textele fiind egal autentice. În cazul divergențelor de interpretare, textul în limba engleză va prevala.

PENTRU  
ROMÂNIA



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

PENTRU  
REPUBLICA PORTUGHEZĂ



ALEXANDRE VASSALO  
Ambasadorul Portugaliei



ACORDO DE SEGURANÇA

ENTRE

A ROMÉNIA

E

A REPÚBLICA PORTUGUESA

SOBRE PROTECÇÃO MÚTUA DE INFORMAÇÃO CLAFISSICADA



Entre as República Portuguesa,  
e as Partes designadas por "Partes";

considerando a necessidade de salvaguardar a Informação Classificada trocada entre as Partes através dos seus órgãos estatais ou outras entidades públicas e privadas que tenham Informação Classificada da outra Parte;

desse modo estabelecer um conjunto de normas sobre a protecção mútua de Informação Classificada trocada entre as Partes,  
concordando seguinte:

## ARTIGO 1.º OBJECTO

O presente Acordo de Segurança, doravante referido como o "Acordo", estabelece as regras de segurança aplicáveis a todos os acordos ou contratos de cooperação, que visem a troca de Informação Classificada, concluídos ou a concluir entre órgãos estatais ou outras entidades públicas e privadas das Partes, devidamente autorizadas para o efeito.

## ARTIGO 2.º ÂMBITO DE APLICAÇÃO

1. O presente Acordo constitui a base jurídica para qualquer actividade que envolva a troca de Informação Classificada entre as Partes, relativamente a casos como:

- a) Cooperação entre as Partes em matéria de defesa nacional e outras questões relacionadas com a segurança nacional;
- b) Cooperação, consórcios, contratos ou qualquer outra relação entre órgãos estatais ou outras entidades públicas ou privadas das Partes relativos à defesa nacional ou a qualquer outra questão relacionada com a segurança nacional;
- c) Vendas de equipamento, produtos e conhecimentos especializados.

2. Nenhuma das Partes pode invocar o presente Acordo de modo a obter Informação Classificada que a outra Parte tenha recebido de uma Terceira Parte.



### ARTIGO 3.º DEFINIÇÕES

Para os efeitos do presente Acordo:

- a) **“Informação Classificada”** designa toda a informação, documento ou material, independentemente da sua forma física, à qual é atribuída uma determinada Classificação de Segurança, de acordo com o respectivo Direito vigente, e que deve ser protegida em conformidade;
- b) **“Documento Classificado”** designa qualquer tipo de registo que contenha Informação Classificada independentemente das suas características físicas, incluindo, sem limitação, itens escritos ou impressos, cartões e fitas de processamento de dados, mapas, tabelas, fotografias, quadros, desenhos, gravações, esboços, notas e papéis de trabalho, duplicados e fita tintada ou reproduções produzidas por quaisquer outros meios ou processos, e registos de som, de voz, magnético, electrónico, óptico ou de vídeo, em qualquer forma, bem como equipamento portátil de processamento automático de dados, com meios de armazenamento de dados residentes em computador e meios de armazenamento de dados em computador amovíveis;
- c) **“Material Classificado”** designa qualquer objecto ou item de maquinaria, protótipo, equipamento, arma ou similar, fabricado à mão ou mecanicamente, produzido ou em processo de fabrico, ao qual foi atribuído uma Classificação de Segurança;
- d) **“Classificação de Segurança”** designa a atribuição de uma classe ou nível de classificação de acordo com o respectivo Direito vigente das Partes;
- e) **“Contrato Classificado”** designa um acordo entre dois ou mais contratantes que estabelece e define os seus direitos e obrigações, e que contém ou implica acesso a Informação Classificada;
- f) **“Contratante ou Subcontratante”** designa uma pessoa individual ou colectiva que tenha capacidade jurídica para celebrar Contratos Classificados;
- g) **“Quebra de Segurança”** designa um acto ou uma omissão contrário ao respectivo Direito vigente das Partes, que comprometa ou que possa comprometer Informação Classificada;

h) **“Comprometimento da Informação Classificada”** designa uma situação em que, devido a uma Quebra de Segurança ou actividade adversa, a Informação Classificada perdeu a sua confidencialidade, integridade ou disponibilidade, ou em que os serviços e recursos de apoio perderam a sua integridade ou disponibilidade, incluindo perda, divulgação parcial ou total, modificação não autorizada e destruição ou negação do serviço;

i) **“Carta de Aspectos de Segurança”** designa um documento emitido pela autoridade competente que integra um Contrato Classificado ou subcontrato e que identifica os requisitos de segurança ou aqueles elementos do contrato que exigem protecção de segurança;

j) **“Lista de Verificação de Classificação de Segurança”** designa uma listagem de Informação Classificada, materiais e actividades relacionadas com um Contrato Classificado, bem como a sua Classificação de Segurança, incluída na Carta de Aspectos de Segurança;

k) **“Certificado de Credenciação de Segurança do Pessoal”** designa um documento a certificar que o titular pode ter acesso a Informação Classificada de uma determinada Classificação de Segurança, em conformidade com o princípio de Necessidade de Conhecer;

l) **“Certificado de Credenciação de Segurança Industrial”** designa um documento a certificar que um organismo está autorizado a efectuar actividades industriais que exijam acesso a Informação Classificada de uma determinada Classificação de Segurança;

m) **“Necessidade de Conhecer”** designa um princípio pelo qual apenas pode ser concedido acesso individual a Informação Classificada àquelas pessoas que, no cumprimento das suas funções, têm necessidade de trabalhar com essa informação ou a ela ter acesso;

n) **“Autoridade de Segurança Competente”** designa a instituição que possui autoridade a nível nacional que, em conformidade com o respectivo Direito vigente das Partes, assegura a implementação uniforme das medidas protectoras de Informação Classificada;

o) **“Autoridade de Segurança Designada”** designa uma instituição que, em conformidade com o respectivo Direito vigente das Partes e coordenada pela Autoridade de Segurança Competente no que respeita à protecção de Informação Classificada, está autorizada a estabelecer, para o seu campo de actividade e de acordo com as suas competências, as suas próprias estruturas e medidas;

- p) “Parte Transmissora” designa a Parte que transmite Informação Classificada à outra Parte;
- q) “Parte Destinatária” designa a Parte que recebe a Informação Classificada transmitida pela Parte Transmissora;
- r) “Terceira Parte” designa qualquer organização internacional ou Estado que não é Parte no presente Acordo.

#### ARTIGO 4.º

#### AUTORIDADES DE SEGURANÇA COMPETENTES

1. As Autoridades de Segurança Competentes responsáveis, a nível nacional, pela implementação e controlo das medidas estipuladas no presente Acordo, são:

Pela Roménia:

Guvernul României  
Oficiul Registrului Național al Informațiilor  
Secrete de Stat  
București — Str. Mureș nr. 4, Sect.1  
Roménia

Pela República Portuguesa:

Autoridade Nacional de Segurança  
Presidência do Conselho de Ministros  
Rua da Junqueira, 69  
1300-342 Lisboa  
Portugal

2. De modo a manter os mesmos padrões de segurança, cada Autoridade de Segurança Competente deverá fornecer, mediante pedido, à outra Autoridade de Segurança Competente, informação sobre a sua organização de segurança, procedimentos e respectivo Direito vigente que regula a protecção de Informação Classificada.

3. De modo a garantir uma estreita cooperação na aplicação do presente Acordo, as Autoridades de Segurança Competentes podem auxiliar-se mutuamente e realizar consultas sempre que solicitado por uma delas.

**ARTIGO 5.º**  
**EQUIVALÊNCIA DAS CLASSIFICAÇÕES DE SEGURANÇA**

As Partes acordam que a equivalência das suas Classificações de Segurança nacionais é a seguinte:

Roménia	República Portuguesa	Equivalente em Inglês
STRICT SECRET DE IMPORTANTĂ DEOSEBITĂ	MUITO SECRETO	TOP SECRET
STRICT SECRET	SECRETO	SECRET
SECRET	CONFIDENCIAL	CONFIDENTIAL
SECRET DE SERVICIU	RESERVADO	RESTRICTED

**ARTIGO 6.º**  
**PROTECÇÃO DA INFORMAÇÃO CLASSIFICADA**

1. A protecção e uso da Informação Classificada trocada entre as Partes são regulados pelas seguintes normas:

a) A Parte Destinatária assegura a toda a Informação Classificada trocada, recebida, produzida ou desenvolvida a mesma protecção conferida à sua própria Informação Classificada com a Classificação de Segurança equivalente;

b) O acesso à Informação Classificada deverá restringir-se às pessoas que, para executarem as suas funções, necessitem de ter acesso à Informação Classificada segundo o princípio da Necessidade de Conhecer e que possuam os Certificados de Credenciação de Segurança do Pessoal apropriados para acesso a informação classificada como CONFIDENCIAL / SECRET/ CONFIDENTIAL ou superior;

c) Os representantes de uma Parte têm acesso a informação classificada como RESERVADO / SECRET DE SERVICIU / RESTRICTED da outra Parte segundo o princípio Necessidade de Conhecer, desde que cumpram os requisitos para acesso a essa Informação Classificada de acordo com o Direito vigente da Parte que representam.

A Parte Destinatária marcará a Informação Classificada recebida com a sua própria marca de Classificação de Segurança, em conformidade com as equivalências referidas no Artigo 5.º do presente Acordo.

3. A Parte Transmissora informará a Parte Destinatária de quaisquer alterações na Classificação de Segurança da Informação Classificada transmitida.

4. A Parte Destinatária não poderá baixar o grau de Classificação de Segurança ou desclassificar a Informação Classificada recebida sem a prévia autorização escrita da Parte Transmissora.

5. As traduções e reproduções de Informação Classificada devem ser feitas de acordo com os seguintes procedimentos:

a) As pessoas envolvidas deverão ser titulares dos Certificados de Credenciação de Segurança do Pessoal apropriados;

b) As traduções e as reproduções serão marcadas e protegidas da mesma forma que a Informação Classificada original;

c) As traduções e o número de cópias a efectuar deverão ser limitadas às requeridas para uso oficial;

d) As traduções deverão ter a indicação, na língua para que foram traduzidas, de que contêm Informação Classificada recebida da Parte Transmissora.

6. A Informação Classificada marcada como STRICT SECRET DE IMPORTANTĂ DEOSEBITĂ / MUITO SECRETO / TOP SECRET apenas poderá ser traduzida ou reproduzida com autorização escrita da Autoridade de Segurança Competente da Parte Transmissora, em conformidade com o respectivo Direito vigente.

7. A Informação Classificada marcada como STRICT SECRET DE IMPORTANTĂ DEOSEBITĂ / MUITO SECRETO / TOP SECRET não poderá ser destruída, devendo ser devolvida à Parte Transmissora.

8. Para a destruição de Informação Classificada marcada como STRICT SECRET / SECRETO / SECRET e SECRET / CONFIDENCIAL / CONFIDENTIAL é necessária a prévia autorização escrita da Parte Transmissora.

9. No caso de uma situação que impossibilite a protecção e devolução de Informação Classificada produzida ou transmitida de acordo com o presente Acordo, a Informação Classificada será destruída imediatamente. A Parte Destinatária informará a Parte Transmissora acerca da destruição da Informação Classificada com a maior brevidade possível.

**ARTIGO 7.º**  
**TRANSMISSÃO DE INFORMAÇÃO CLASSIFICADA**

1. A Informação Classificada será transmitida por via diplomática, correio militar ou outros meios aprovados pelas Autoridades de Segurança Competentes.
2. Se existir Informação Classificada de grande volume a ser transmitida, as Autoridades de Segurança Competentes devem acordar mutuamente os meios de transporte, a rota e as medidas de segurança para cada caso.
3. A troca de Informação Classificada através de sistemas de informação e comunicação protegidos ocorrerá em conformidade com os procedimentos de segurança mutuamente acordados pelas Autoridades de Segurança Competentes das Partes.
4. A Parte Destinatária confirmará, por escrito, a recepção da Informação Classificada.

**ARTIGO 8.º**  
**DIVULGAÇÃO DE INFORMAÇÃO**

1. A divulgação de Informação Classificada a uma Terceira Parte ou a qualquer entidade pública ou privada da nacionalidade de um terceiro Estado apenas poderá ocorrer com a prévia autorização escrita da Autoridade de Segurança Competente da Parte Transmissora, que poderá impor outras limitações à divulgação.
2. Cada Parte deve assegurar que a Informação Classificada recebida da outra Parte é usada para os fins para os quais foi divulgada.

**ARTIGO 9.º**  
**PROCEDIMENTOS DE CREDENCIAÇÃO DE SEGURANÇA**

1. Cada Parte reconhecerá os Certificados de Credenciação de Segurança do Pessoal e os Certificados de Credenciação de Segurança Industrial emitidos de acordo com o Direito vigente da outra Parte.



2. As Autoridades de Segurança Competentes informar-se-ão mutuamente sobre quaisquer alterações relativas aos Certificados de Credenciação de Segurança do Pessoal e aos Certificados de Credenciação de Segurança Industrial.

3. Se solicitado, as Autoridades de Segurança Competentes das Partes, tendo em consideração o respectivo Direito vigente, colaborarão no decurso dos procedimentos para a credenciação de segurança dos seus nacionais que residam no território da outra Parte ou das instalações que ali estejam localizadas, precedendo a emissão do Certificado de Credenciação de Segurança do Pessoal e do Certificado de Credenciação de Segurança Industrial.

### ARTIGO 10.º CONTRATOS CLASSIFICADOS

1. No caso de Contratos Classificados a serem concluídos e executados no território de uma das Partes, a Autoridade de Segurança Competente da outra Parte deverá obter garantia prévia, por escrito, de que o Contratante proposto possui um Certificado de Credenciação de Segurança Industrial de nível apropriado.

2. O Contratante compromete-se a:

- a) Assegurar que as suas instalações dispõem das condições adequadas para processar a Informação Classificada;
- b) Obter o Certificado de Credenciação de Segurança Industrial apropriado para aquelas instalações;
- c) Assegurar que as pessoas que desempenhem funções que exijam acesso à Informação Classificada estão habilitadas com o Certificado de Credenciação de Segurança do Pessoal apropriado;
- d) Assegurar que todas as pessoas que têm acesso à Informação Classificada estão informadas sobre a sua responsabilidade relativa à protecção da Informação Classificada, de acordo com o Direito vigente;
- e) Permitir inspecções de segurança às suas instalações por representantes das Autoridades de Segurança Competentes.

3. Qualquer Subcontratante deverá cumprir as mesmas obrigações de segurança que o Contratante.

4. A Autoridade de Segurança Competente será responsável pela supervisão e controlo do cumprimento dos requisitos estabelecidos no número 2 do presente Artigo por parte do Contratante.



5. Qualquer Contrato Classificado celebrado entre Contratantes das Partes, nos termos do presente Acordo, deverá incluir uma Carta de Aspectos de Segurança apropriada identificando, pelo menos, os seguintes aspectos:

- a) Lista de Verificação de Classificação de Segurança;
- b) Procedimento para a comunicação de alterações na Classificação de Segurança;
- c) Canais de comunicação e meios para a transmissão electromagnética;
- d) Procedimento para o transporte de Informação Classificada;
- e) Autoridades competentes pela coordenação e salvaguarda da Informação Classificada relacionada com o Contrato;
- f) Obrigatoriedade de notificação de qualquer Comprometimento ou suspeita de Comprometimento de Informação Classificada.

6. Deverá ser enviada cópia da Carta de Aspectos de Segurança de qualquer Contrato Classificado à Autoridade de Segurança Competente da Parte em cujo território o Contrato Classificado será executado, de forma a garantir a adequada supervisão e controlo de segurança.

7. As Autoridades de Segurança Competentes podem acordar visitas mútuas com o objectivo de analisarem a eficácia das medidas adoptadas por um Contratante para a protecção de Informação Classificada envolvidas num Contrato Classificado. A notificação da visita deverá ser efectuada com uma antecedência mínima de vinte dias úteis.

## ARTIGO 11.º VISITAS

1. As visitas que envolvam acesso a Informação Classificada por nacionais de uma Parte à outra Parte estão sujeitas à prévia autorização escrita conferida pelas Autoridades de Segurança Competentes ou Autoridades de Segurança Designadas em conformidade com o respectivo Direito vigente.

2. O pedido de visita deve ser submetido através da Autoridade de Segurança Competente da Parte anfitriã.

3. As visitas que envolvam acesso a Informação Classificada serão autorizadas por uma Parte aos visitantes da outra Parte apenas se estes:

- a) Possuírem um Certificado de Credenciação de Segurança do Pessoal; e
- b) Estiverem autorizados a receber ou ter acesso a Informação Classificada segundo o princípio da Necessidade de Conhecer, em conformidade com o respectivo Direito vigente.



4. A Autoridade de Segurança Competente da Parte visitante notificará a Autoridade de Segurança Competente da Parte anfitriã da visita planeada através de um pedido de visita, o qual deve ser recebido com pelo menos vinte dias úteis de antecedência.

5. Em casos urgentes, o pedido de visita será transmitido com pelo menos cinco dias úteis de antecedência.

6. A Autoridade de Segurança Competente da Parte que recebe o pedido de visita informará, em tempo oportuno, a Autoridade de Segurança Competente da Parte requerente sobre a decisão.

7. As visitas de pessoas de uma Terceira Parte que envolvam acesso a Informação Classificada da Parte Transmissora estão sujeitas à prévia autorização escrita conferida pela Autoridade de Segurança Competente ou pela Autoridade de Segurança Designada, em conformidade com o respectivo Direito vigente.

8. Uma vez aprovada a visita, a Autoridade de Segurança Competente ou Autoridade de Segurança Designada da Parte anfitriã fornecerá uma cópia do pedido de visita ao oficial de segurança do estabelecimento, instalação ou organização a ser visitada.

9. A validade da autorização de visita não excederá os doze meses.

10. Para qualquer Contrato Classificado, as Partes podem acordar elaborar listas de pessoas autorizadas a efectuar visitas recorrentes. Essas listas são válidas por um período inicial de doze meses.

11. Após a aprovação dessas listas pelas Partes, os termos de cada visita serão directamente acordados entre os representantes apropriados das entidades envolvidas, nos termos e condições do presente Acordo.

12. O pedido de visita deverá incluir:

a) O nome e o apelido do visitante, data e local de nascimento, nacionalidade e o número do passaporte ou bilhete de identidade;

b) O nome do estabelecimento, instalação ou organização que o visitante representa ou a que pertence;

c) O nome e morada do estabelecimento, instalação ou organização a visitar;

d) Confirmação do Certificado de Credenciação de Segurança do Pessoal do visitante e a respectiva validade;

e) Objecto e propósito da visita ou visitas;

f) A data prevista para a visita ou visitas e a respectiva duração, e, em caso de visitas recorrentes, deverá ser referido o período total das visitas;

- g) O nome e número de telefone do ponto de contacto no estabelecimento, instalação ou organização a visitar, contactos anteriores e qualquer outra informação útil para determinar a justificação da visita ou visitas;
- h) A data, a assinatura e a aposição do selo oficial da Autoridade de Segurança Competente ou da Autoridade de Segurança Designada apropriada.

## **ARTIGO 12.º** **QUEBRA DE SEGURANÇA**

1. Em caso de Quebra de Segurança relacionada com a Informação Classificada transmitida ou recebida da outra Parte, a Autoridade de Segurança Competente da Parte onde ocorra a Quebra de Segurança informará a Autoridade de Segurança Competente da outra Parte, com a brevidade possível, e instaurará a correspondente investigação.
2. Se a Quebra de Segurança ocorrer num Terceiro Estado, a Autoridade de Segurança Competente da Parte Transmissora adoptará as medidas previstas no número 1 do presente Artigo.
3. A outra Parte deverá, se necessário, cooperar na investigação.
4. Em qualquer caso, a outra Parte será informada, por escrito, dos resultados e conclusões da investigação, incluindo as razões da Quebra de Segurança, a extensão dos danos e as medidas adoptadas para a sua limitação.

## **ARTIGO 13.º** **ENCARGOS**

Cada Parte assumirá os encargos que para si advenham da aplicação e supervisão de todos os aspectos do presente Acordo.

## **ARTIGO 14.º** **RESOLUÇÃO DE CONTROVÉRSIAS**

Qualquer controvérsia sobre a interpretação ou a aplicação do presente Acordo, se não resolvido através de consultas entre as Autoridades de Segurança Competentes, será resolvido através de negociação, por via diplomática.

## ARTIGO 15.º ENTRADA EM VIGOR

O presente Acordo entrará em vigor no trigésimo dia após a recepção da última das notificações, por escrito e por via diplomática, de que foram cumpridos todos os requisitos de Direito interno de ambas as Partes.

## ARTIGO 16.º REVISÃO

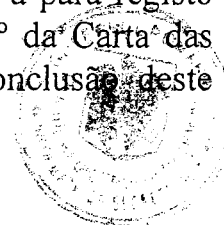
1. O presente Acordo pode ser objecto de revisão com base no mútuo consentimento escrito de ambas as Partes.
2. As emendas entrarão em vigor nos termos previstos no Artigo 15.º do presente Acordo.

## ARTIGO 17.º VIGÊNCIA E DENÚNCIA

1. O presente Acordo permanecerá em vigor por um período de tempo ilimitado.
2. Qualquer uma das Partes pode, a qualquer momento, denunciar o presente Acordo.
3. A denúncia deverá ser notificada, por escrito e por via diplomática, produzindo efeitos seis meses após a data da recepção da respectiva notificação.
4. Não obstante a denúncia, toda a Informação Classificada recebida em conformidade com o presente Acordo continuará a ser protegida de acordo com as disposições do mesmo, até que a Parte Transmissora dispense a Parte Destinatária dessa obrigação.

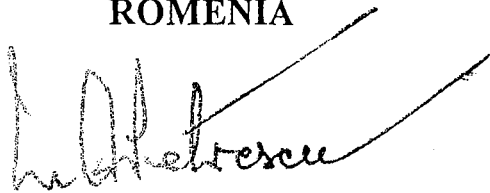
## ARTIGO 18.º REGISTO

A Parte em cujo território o presente Acordo for assinado submetê-lo-á para registo junto do Secretariado das Nações Unidas, nos termos do artigo 102.º da Carta das Nações Unidas, devendo, igualmente, notificar a outra Parte da conclusão deste procedimento e indicar o número de registo atribuído.



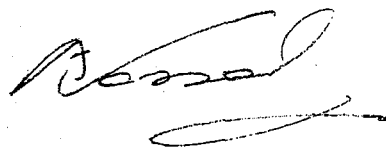
Assinado em Bucareste a 14 de Maio de 2008, em duplicado, nas línguas romena, portuguesa e inglesa, sendo os três textos igualmente autênticos. Em caso de divergência de interpretação prevalecerá a versão em língua inglesa.

PELA  
ROMÉNIA



**Prof. Dr. MARIUS PETRESCU**  
Secretário de Estado  
Director Geral do Ofício  
do Registo Nacional das Informações  
Secretas de Estado

PELA  
REPÚBLICA PORTUGUESA



**ALEXANDRE VASSALO**  
Embaixador de Portugal

*Conf. de registo  
Nacional*

**SECURITY AGREEMENT**

**BETWEEN**

**ROMANIA**

**AND**

**THE PORTUGUESE REPUBLIC**

**ON THE MUTUAL PROTECTION OF CLASSIFIED INFORMATION**

Romania and the Portuguese Republic,

Hereinafter called the Parties,

Considering the need to safeguard the Classified Information exchanged between them through their state bodies or other legal public and private entities which deal with Classified Information of the other Party;

Desiring to create a set of rules on the mutual protection of Classified Information exchanged between the Parties,

Agree as follows:

## ARTICLE 1 OBJECT

This Security Agreement, hereinafter referred to as Agreement, establishes the security rules applicable to all co-operation arrangements or contracts, which envisage the exchange of Classified Information, concluded or to be concluded between state bodies or other legal public and private entities of the Parties, duly authorized to that purpose.

## ARTICLE 2 SCOPE OF APPLICATION

This Agreement forms the legal basis of any activity, involving the exchange of Classified Information between the Parties, concerning cases such as:

- a co-operation between the Parties concerning the national defense and any other issue related to national security;
- b co-operation, joint ventures, contracts or any other relation between state bodies or other public or private entities of the Parties in the field of national defense and any other issue related to national security;

- c. sales of equipment, products and know-how.
- 2. Either Party may not invoke this Agreement in order to obtain Classified Information that the other Party has received from a Third Party.

### ARTICLE 3 DEFINITIONS

For the purpose of this Agreement:

- a) **Classified Information** means any information, document or material, regardless of its physical form, to which a particular Security Classification has been assigned in compliance with the respective Law in force and which shall be protected accordingly;
- b) **Classified Document** means any sort of record containing Classified Information regardless of its form or physical characteristics, including, without limitation, written or printed matters, data processing cards and tapes, maps, charts, photographs, paintings, drawings, engravings, sketches, working notes and papers, carbon copies and ink ribbons, or reproductions produced by any means or processes, and sound, voice, magnetic or electronic or optical or video recordings in any form, and portable automated data processing equipment with resident computer storage media, and removable computer storage media;
- c) **Classified Material** means any object or item of machinery, prototype, equipment, weapon, or similar, mechanically or hand made, manufactured or in process of manufacture, to which a Security Classification has been assigned;
- d) **Security Classification** means the assignment of a class or level of classification in accordance with the respective Law in force of the Parties;
- e) **Classified Contract** means an arrangement between two or more contractors establishing and defining their rights and obligations and containing or implying access to Classified Information;
- f) **Contractor or Sub-Contractor** means an individual or legal entity possessing the legal capacity to conclude Classified Contracts;



- g) **Breach of Security** means an act or an omission contrary to the respective Law in force of the Parties, that results in an actual or possible Compromise of Classified Information;
- h) **Compromise of Classified Information** means a situation when, due to a Breach of Security or adverse activity, Classified Information has lost its confidentiality, integrity or availability, or when supporting services and resources have lost their integrity or availability, including loss, partial or total disclosure, unauthorized modification and destruction or denial of service;
- i) **Security Aspects Letter** means a document issued by the appropriate authority as a part of any Classified Contract or sub-contract, identifying the security requirements or those elements of the contract requiring security protection;
- j) **Security Classification Check-List** means a listing of Classified Information, materials and activities related to a Classified Contract and their Security Classification, included in the Security Aspects Letter;
- k) **Personnel Security Clearance Certificate** means a document certifying that the holder may have access to Classified Information of a certain Security Classification, in compliance with the Need-to-Know principle;
- l) **Facility Security Clearance Certificate** means a document certifying that a legal body is authorized to carry out industrial activities requiring access to Classified Information of a certain Security Classification;
- m) **Need-to-Know** means a principle by which access to Classified Information may be granted individually, only to those persons who, in performing their duties, need to work with or have access to such information;
- n) **Competent Security Authority** means the institution empowered with authority at national level which, in compliance with the respective Law in force of the Parties, ensures the unitary implementation of the protective measures for Classified Information;
- o) **Designated Security Authority** means the institution which, in compliance with the respective Law in force of the Parties, coordinated by the Competent Security Authority in the field of the protection of Classified Information, is empowered to establish, for its activity field and according to its competences, its own structures and measures;



- p) **Originating Party** means the Party which transmits Classified Information to the other Party;
- q) **Receiving Party** means the Party that receives the Classified Information transmitted to it by the Originating Party;
- r) **Third Party** means any international organisation or state that is not a Party to this Agreement.

**ARTICLE 4**  
**COMPETENT SECURITY AUTHORITIES**

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

<p>For Romania:</p> <p>Guvernul României</p> <p>Oficiul Registrului Național al</p> <p>Informațiilor Secrete de Stat</p> <p>București – Str. Mureș nr. 4, Sect.1</p> <p>ROMÂNIA</p>	<p>For the Portuguese Republic:</p> <p>Autoridade Nacional de Segurança</p> <p>Presidência do Conselho de Ministros</p> <p>Rua da Junqueira, 69</p> <p>1300-342 Lisboa</p> <p>PORTUGAL</p>
---	--

2. In order to keep the same security standards, each Competent Security Authority shall provide, upon request, to the other Competent Security Authority, information about its security organization, procedures and the respective Law in force regulating the protection of Classified Information.
3. In order to ensure close co-operation in the implementation of this Agreement, Competent Security Authorities may assist each other and may hold consultations on the request made by one of them.

**ARTICLE 5**  
**EQUIVALENCE OF THE SECURITY CLASSIFICATIONS**

The Parties agree that the equivalence of their national Security Classifications is the following:

<b>Romania</b>	<b>Portuguese Republic</b>	<b>English Equivalent</b>
STRICT SECRET DE IMPORTANTĂ DEOSEBITĂ	MUITO SECRETO	TOP SECRET
STRICT SECRET	SECRETO	SECRET
SECRET	CONFIDENCIAL	CONFIDENTIAL
SECRET DE SERVICIU	RESERVADO	RESTRICTED

**ARTICLE 6**  
**PROTECTION OF CLASSIFIED INFORMATION**

1. The protection and use of the Classified Information exchanged between the Parties are regulated by the following rules:
  - a) the Receiving Party shall ensure to all the exchanged, received, produced or developed Classified Information the same protection as it is provided for its own Classified Information with the equivalent Security Classification;
  - b) the access to Classified Information shall be restricted to persons who, in order to perform their functions, need to have access to the Classified Information on a Need-to-Know basis and hold appropriate Personnel Security Clearance Certificates for access to information classified SECRET / CONFIDENCIAL / CONFIDENTIAL or above;
  - c) representatives of a Party have access to information classified SECRET DE SERVICIU / RESERVADO / RESTRICTED of the other Party on a Need-to-Know basis, provided they meet the requirements for access to such Classified Information according to the Law in force of the Party they represent.
2. The Receiving Party shall mark the received Classified Information with its own equivalent Security Classification marking, in accordance with the equivalences referred to in Article 5 of this Agreement.

3. The Originating Party shall inform the Receiving Party of any changes in Security Classification of the transmitted Classified Information.
4. The Receiving Party shall neither downgrade nor declassify the received Classified Information without the prior written consent of the Originating Party.
5. Translations and reproductions of Classified Information shall be made according to the following procedures:
  - a) the individuals shall hold the appropriate Personnel Security Clearance Certificates;
  - b) the translations and the reproductions shall be marked and placed under the same protection as the original Classified Information;
  - c) the translations and the number of reproductions shall be limited to that required for official purposes;
  - d) the translations shall bear an appropriate note in the language into which it is translated indicating that it contains Classified Information received from the Originating Party.
6. Classified Information marked as STRICT SECRET DE IMPORTANTĂ DEOSEBITĂ / MUITO SECRETO / TOP SECRET shall be translated or reproduced only upon the written permission of the Competent Security Authority of the Originating Party, in accordance with the respective Law in force.
7. Classified Information marked as STRICT SECRET DE IMPORTANTĂ DEOSEBITĂ/ MUITO SECRETO / TOP SECRET shall not be destroyed and it shall be returned to the Originating Party.
8. For the destruction of Classified Information marked as STRICT SECRET / SECRETO / SECRET and SECRET / CONFIDENCIAL/ CONFIDENTIAL prior written consent of the Originating Party is required.
9. In case of a situation that makes it impossible to protect and return Classified Information generated or transmitted according to this Agreement, the Classified Information shall be destroyed immediately. The Receiving Party shall notify the Originating Party about the destruction of the Classified Information as soon as possible.

**ARTICLE 7**  
**TRANSMISSION OF CLASSIFIED INFORMATION**

1. Classified Information shall be transmitted by diplomatic channels, military couriers or other means approved by the Competent Security Authorities.
2. If a large consignment containing Classified Information is to be transmitted, the Competent Security Authorities shall mutually agree on the means of transportation, the route and security measures for each case.
3. The exchange of Classified Information through protected information and communication systems shall take place in accordance with the security procedures mutually agreed on by the Competent Security Authorities of the Parties.
4. The Receiving Party shall confirm in writing the receipt of the Classified Information.

**ARTICLE 8**  
**RELEASE OF INFORMATION**

1. Release of Classified Information to Third Parties or to any public and private entity which holds the nationality of a third state can take place after written consent of the Competent Security Authority of the Originating Party, which may impose further limitations to the release.
2. Each Party shall ensure that Classified Information received from the other Party is used for the purpose for which such information has been released.

**ARTICLE 9**  
**SECURITY CLEARANCE PROCEDURES**

1. Each Party shall recognize the Personnel Security Clearance Certificates and Facility Security Clearance Certificates issued in accordance with the Law in force of the other Party.

2. The Competent Security Authorities shall inform each other about any modifications regarding the Personnel Security Clearance Certificates and Facility Security Clearance Certificates.
3. On request, the Competent Security Authorities of the Parties, taking into account their respective Law in force, shall assist each other during the clearance procedures of their nationals living or facilities located in the territory of the other Party, preceding the issue of the Personnel Security Clearance Certificates and the Facility Security Clearance Certificates.

## ARTICLE 10 CLASSIFIED CONTRACTS

1. In case of Classified Contracts to be concluded and implemented in the territory of one of the Parties, the Competent Security Authority of the other Party shall obtain prior written assurance that the proposed Contractor holds a Facility Security Clearance Certificate of an appropriate level.
2. The Contractor commits itself to:
  - a) ensure that its premises have adequate conditions for the processing of Classified Information;
  - b) have an appropriate Facility Security Clearance Certificate granted to those premises;
  - c) have appropriate Personnel Security Clearance Certificates granted to persons who perform functions that require access to Classified Information;
  - d) ensure that all persons having access to Classified Information are informed of their responsibility towards the protection of Classified Information, according to the Law in force;
  - e) allow security inspections of its premises by representatives of the Competent Security Authorities.
3. Any Sub-Contractor must fulfill the same security obligations as the Contractor.
4. The Competent Security Authority shall be responsible for the supervision and control of the compliance of the Contractor with the commitments set in paragraph 2 of this Article.
5. Every Classified Contract concluded between Contractors of the Parties, under the provisions of this Agreement, shall include an appropriate Security Aspects Letter identifying at least the following aspects:

- a) Security Classification Check-List;
  - b) procedure for the communication of changes in the Security Classification;
  - c) communication channels and means for electromagnetic transmission;
  - d) procedure for the transportation of Classified Information;
  - e) authorities competent for the co-ordination of the safeguarding of Classified Information related to the Contract;
  - f) an obligation to notify any actual or suspected Compromise of Classified Information.
6. A copy of the Security Aspects Letter of any Classified Contract shall be forwarded to the Competent Security Authority of the Party where the Classified Contract is to be performed in order to allow adequate security supervision and control.
7. The Competent Security Authorities may agree on mutual visits in order to analyse the efficiency of the measures adopted by a Contractor for the protection of Classified Information involved in a Classified Contract. Notice of the visit shall be provided at least twenty working days in advance.

## ARTICLE 11 VISITS

1. Visits entailing access to Classified Information by nationals from one Party to the other Party are subject to prior written authorisation given by the Competent Security Authorities or Designated Security Authorities according to the respective Law in force.
2. The request for visit shall be submitted through the Competent Security Authority of the host Party.
3. Visits entailing access to Classified Information shall be allowed by one Party to visitors from the other Party only if they:
  - a) hold appropriate Personnel Security Clearance Certificates; and
  - b) have been authorised to receive or to have access to Classified Information on a Need-to-Know basis, in accordance with the respective Law in force.
4. The Competent Security Authority of the Party requesting the visit shall notify the Competent Security Authority of the host Party of the planned visit through a request for visit, which has to be received at least twenty working days in advance.

5. In urgent cases, the request for visit shall be transmitted at least five working days in advance.
6. The Competent Security Authority of the Party that receives the request for visit shall inform, in due time, the Competent Security Authority of the requesting Party about the decision.
7. Visits of individuals from a Third Party entailing access to Classified Information of the Originating Party shall only be authorized by a written consent given by the Competent Security Authority or Designated Security Authority in accordance with the respective Law in force.
8. Once the visit has been approved, the Competent Security Authority or Designated Security Authority of the host Party shall provide a copy of the request for visit to the security officer of the establishment, facility or organisation to be visited.
9. The validity of the visit authorisation shall not exceed twelve months.
10. For any Classified Contract the Parties may agree to establish lists of authorized persons to make recurring visits. Those lists are valid for an initial period of twelve months.
11. Once those lists have been approved by the Parties, further details of the specific visits shall be directly arranged between the appropriate representatives of the entities involved, according to the terms and conditions agreed upon.
12. The request for visit shall include:
  - a) visitor's first and last name, place and date of birth, nationality, passport or identification card number;
  - b) name of the establishment, facility or organisation the visitor represents or belongs to;
  - c) name and address of the establishment, facility or organisation to be visited;
  - d) confirmation of the visitor's Personnel Security Clearance Certificate and its validity;
  - e) object and purpose of the visit or visits;
  - f) expected date and duration of the requested visit or visits, and in case of recurring visits, the total period covered by the visits should be stated;
  - g) name and phone number of the point of contact at the establishment, facility or organisation to be visited, previous contacts and any other information useful to determine the justification of the visit or visits;



h) The date, signature and stamping of the official seal of the Competent Security Authority or of the appropriate Designated Security Authority.

## **ARTICLE 12 BREACH OF SECURITY**

1. In case of Breach of Security related with Classified Information originated by or received from the other Party, the Competent Security Authority of the Party where the Breach of Security has occurred shall inform the Competent Security Authority of the other Party, as soon as possible, and ensure the appropriate investigation.
2. If a Breach of Security occurs in a third state, the Competent Security Authority of the dispatching Party shall take the actions stipulated in paragraph 1 of the present Article.
3. The other Party shall, if required, co-operate in the investigation.
4. In any case, the other Party shall be informed, in writing, of the results and the conclusions of the investigation, including the reasons for the Breach of Security, the extent of the damage and the respective measures taken to limit it.

## **ARTICLE 13 EXPENSES**

Each Party shall bear its own expenses incurred in connection with the application and supervision of all aspects of this Agreement.

## **ARTICLE 14 SETTLEMENT OF DISPUTES**

Any dispute concerning the interpretation or application of this Agreement, if not settled by consultations between the Competent Security Authorities, shall be settled by negotiations through diplomatic channels.



**ARTICLE 15  
ENTRY INTO FORCE**

This Agreement shall enter into force on the thirtieth day following the receipt of the last of the notifications, in writing and through diplomatic channels, stating that all the internal legal procedures of both Parties have been fulfilled.

**ARTICLE 16  
AMENDMENTS**

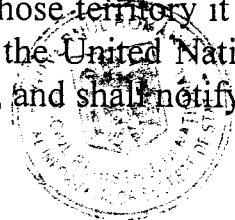
1. Both Parties may amend this Agreement on the basis of mutual written consent.
2. The amendments shall enter into force in accordance with the terms specified in Article 15 of this Agreement.

**ARTICLE 17  
DURATION AND TERMINATION**

1. This Agreement shall remain in force for an indefinite period of time.
2. Each Party may, at any time, terminate this Agreement.
3. The termination shall be notified, in writing and through diplomatic channels and shall become effective six months after the date of receipt of the respective notification.
4. Notwithstanding the termination, all Classified Information received pursuant to this Agreement shall continue to be protected in accordance with the provisions set forth herein, until the Originating Party dispenses the Receiving Party from this obligation.

**ARTICLE 18  
REGISTRATION**

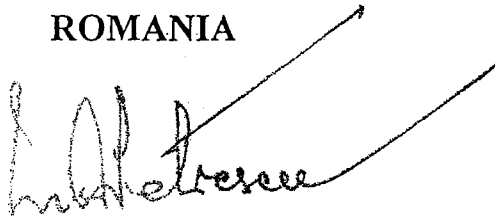
After the entry into force of this Agreement, the Party in whose territory it was signed shall transmit it for registration to the Secretariat of the United Nations according to article 102 of the Charter of the United Nations, and shall notify the



other Party of the conclusion of this proceeding, indicating the respective number of registration.

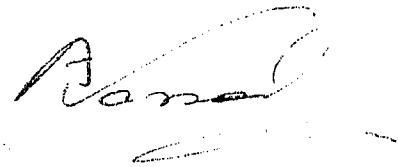
Signed in Bucharest on 14<sup>th</sup> of May 2008 in two originals, each one in the Romanian, Portuguese and English languages, all texts being equally authentic. In case of any divergence of interpretation the English text shall prevail.

**FOR  
ROMANIA**



**Prof. dr. MARIUS PETRESCU**  
**Secretary of State**  
**Director General**  
**of the National Registry Office for**  
**Classified Information**

**FOR  
THE PORTUGUESE REPUBLIC**



**ALEXANDRE VASSALO**  
**Portuguese Ambassador**

*ant cu original  
Petrescu*

