ACORD DE SECURITATE

ÎNTRE

GUVERNUL ROMÂNIEI

ŞI

GUVERNUL REGATULUI NORVEGIEI

PRIVIND PROTECŢIA RECIPROCĂ

A INFORMAŢIILOR CLASIFICATE

Guvernul României şi Guvernul Regatului Norvegiei, denumite în continuare Părţi,

În scopul protecţiei Informaţiilor Clasificate schimbate direct sau prin intermediul persoanelor juridice care gestionează Informaţii Clasificate ale statului celeilalte Părţi şi în cadrul activităţilor care ţin de competenţa Părţilor,

Au convenit următoarele:

ARTICOLUL 1
DISPOZIŢII GENERALE

1. Scopul prezentului Acord este de a asigura protecţia Informaţiilor Clasificate schimbate sau produse în cadrul procesului de cooperare dintre Părţi.

2. Decizia de transmitere sau de schimb de Informaţii Clasificate va fi adoptată în conformitate cu legislaţiile naţionale ale Părţilor.

3. Prezentul Acord acoperă orice tip de activitate şi face parte integrantă din orice contract sau acord ce implică Informaţii Clasificate, care se încheie între Părţi sau persoane juridice din statele Părţilor.

4. Prezentul Acord nu va afecta obligaţiile celor două Părţi ce derivă din alte acorduri internaţionale şi nu va fi folosit împotriva intereselor, securităţii şi integrităţii teritoriale ale altor state.

ARTICOLUL 2
DEFINIŢII

În scopul prezentului Acord:

a. **Informaţie Clasificată** înseamnă:
orice informaţie, document sau material, indiferent de forma fizică a acestora, cărora li s-a atribuit o Clasificare de Securitate în conformitate cu legislaţia naţională respectivă şi care vor fi protejate corespunzător;

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

c. **Material Clasificat** înseamnă:
orice obiect sau parte a unui mecanism, prototip, echipament, armă etc., realizate mecanic sau manual, fabricate sau aflate în curs de fabricație, cărora li s-a atribuit o Clasificare de Securitate;

d. **Clasificare de Securitate** înseamnă:
atribuirea unei clase sau a unui nivel de clasificare în conformitate cu legislațiile naționale ale Părților;

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

f. **Contractor** sau **Sub-Contractor** înseamnă:
o persoană fizică sau persoană juridică având capacitatea legală de a încheia Contracte Clasificate;

g. **Incident de Securitate** înseamnă:
o acțiune sau omisiune contrară legislațiilor naționale ale Părților, care are ca rezultat Compromiterea efectivă sau posibilă a Informațiilor Clasificate;

h. **Compromiterea Informațiilor Clasificate** înseamnă:
o situație în care - datorită unui Incident de Securitate sau unei activități ostile (precum spionaj, act de terorism sau furt) - Informațiile Clasificate și-au pierdut confidențialitatea, integritatea sau disponibilitatea, ori atunci când serviciile sau resursele conexe și-au pierdut integritatea sau disponibilitatea. Aceasta include pierderea, divulgarea parțială sau totală, modificarea și distrugerea neautorizată sau refuzul serviciului;

i. **Anexa de Securitate** înseamnă:
un document emis de către autoritatea competentă ca parte a oricărui Contract Clasificat sau sub-contract clasificat, ce identifică cerințele de securitate sau acele elemente ale contractului ce necesită protecție de securitate;

j. **Lista Clasificărilor de Securitate** înseamnă:
o listă a informațiilor, materialelor şi activităților clasificate aferente unui Contract Clasificat şi Clasificările de Securitate ale acestora, inclusă în Anexa de Securitate;

k. **Certificat de Securitate a Personalului** înseamnă:
un document care atestă faptul că, pentru exercitarea atribuțiilor de serviciu, deținătorul acestuia poate avea acces la Informații Clasificate de o anumită Clasificare de Securitate, conform principiului Necesității de a Cunoaşte, emis în conformitate cu legislațiile naționale ale Părților;

l. **Certificat de Securitate Industrială/Autorizație de Securitate Industrială** înseamnă:
un document care atestă faptul că o persoană juridică este autorizată să desfăşoare activități industriale ce necesită acces la Informații Clasificate, emis în conformitate cu legislațiile naționale ale Părților;

m. **Necesitatea de a Cunoaşte** înseamnă:
principiul conform căruia accesul la Informații Clasificate poate fi acordat, în mod individual, numai acelor persoane care, în îndeplinirea sarcinilor de serviciu, trebuie să lucreze cu astfel de informații sau să aibă acces la ele;

n. **Autoritate Competentă de Securitate** înseamnă:
instituție învestită cu autoritate la nivel național care, în conformitate cu legislațiile Părților, asigură implementarea unitară a măsurilor de protecție a Informațiilor Clasificate. Aceste autorități sunt menționate în articolul 7 al prezentului Acord;

o. **Autoritate Desemnată de Securitate** înseamnă:
instituția care, în conformitate cu legislația națională a fiecărei Părți, este autorizată să stabilească, pentru domeniul său de activitate şi responsabilitate, structuri şi măsuri proprii referitoare la coordonarea şi controlul activității privind protecția Informațiilor Clasificate. Autoritatea Desemnată de Securitate este coordonată, în domeniul protecției Informațiilor Clasificate, de Autoritatea Competentă de Securitate;

p. **Terț** înseamnă:
orice stat, persoană, instituție, organizație națională sau internațională, persoană juridică de drept public sau privat care nu este parte la prezentul Acord.

ARTICOLUL 3
PROTECȚIA INFORMAȚIILOR CLASIFICATE

1. În conformitate cu legislațiile lor naționale, Părțile vor lua măsurile corespunzătoare pentru protecția Informațiilor Clasificate transmise, primite, produse sau elaborate ca rezultat al oricărui acord sau oricărei relații între Părți sau între persoanele juridice ale statelor Părților. Părțile vor asigura pentru Informațiile Clasificate schimbate, primite, produse sau elaborate același nivel de protecție, ca și pentru propriile Informații Clasificate echivalente, conform prevederilor articolului 4 al prezentului Acord.

2. Partea primitoare nu va scădea Clasificarea de Securitate a Informațiilor Clasificate primite și nici nu va declasifica aceste informații fără acordul prealabil scris al Autorității Competente de Securitate a Părții emitente. Autoritatea Competentă de Securitate a Părții emitente va informa Autoritatea Competentă de Securitate a Părții primitoare asupra oricăror modificări survenite în Clasificarea de Securitate a informațiilor schimbate.

3. Multiplicarea sau modificarea Informațiilor Clasificate primite se poate realiza numai dacă Partea emitentă nu prevede în mod expres altfel. Exemplarele multiplicate ale Informațiilor Clasificate vor primi marcaje de Clasificare de Securitate echivalente cu Clasificarea de Securitate a originalului și vor fi protejate în același mod ca și informațiile originale. Numărul exemplarelor se va limita la numărul necesar scopurilor oficiale. Informațiile clasificate STRICT SECRET DE IMPORTANȚĂ DEOSEBITĂ / STRENGT HEMMELIG / TOP SECRET vor fi multiplicate numai cu acordul prealabil scris al Părții emitente.

4. Informațiile și Materialele Clasificate vor fi distruse numai cu acordul scris sau la cererea Părții emitente, în conformitate cu legislațiile naționale ale Părților, astfel încât reconstituirea parțială sau totală a Informațiilor Clasificate să nu fie posibilă. Dacă Partea emitentă nu este de acord cu distrugerea unor Informații Clasificate, Materialul sau Documentul Clasificat îi va fi returnat.
Informațiile STRICT SECRET DE IMPORTANȚĂ DEOSEBITĂ / STRENGT HEMMELIG / TOP SECRET nu vor fi distruse, ci returnate Părții emitente.
În caz de pericol iminent, Informațiile Clasificate vor fi distruse fără autorizare prealabilă. Autoritatea Competentă de Securitate a Părții emitente va fi imediat informată asupra acestui fapt.

5. Partea primitoare va informa Partea emitentă asupra distrugerii Informațiilor Clasificate.

6. Accesul la Informații Clasificate și/sau în locații și incinte unde se desfășoară activități ce implică Informații Clasificate sau unde sunt depozitate Informații Clasificate va fi permis, cu respectarea principiului Necesității de a cunoaște,

numai persoanelor care deţin Certificat de Securitate a Personalului corespunzător Clasificării de Securitate a informaţiilor pentru care se solicită accesul.

7. Fiecare Parte va urmări respectarea legislaţiilor naţionale de către persoanele juridice care deţin, elaborează, produc şi/sau utilizează Informaţii Clasificate ale statului celeilalte Părţi, inclusiv prin vizite de inspecţie.

8. Înainte ca un reprezentant al unei Părţi să furnizeze Informaţii Clasificate unui reprezentant al celeilalte Părţi, Partea primitoare va informa Partea emitentă că reprezentantul său deţine Certificat de Securitate a Personalului corespunzător celei mai înalte Clasificări de Securitate a informaţiilor la care acesta urmează să aibă acces, şi că Informaţiile Clasificate sunt protejate conform prevederilor prezentului Acord.

ARTICOLUL 4
CLASIFICĂRILE DE SECURITATE

1. Clasificările de Securitate aplicabile informaţiilor schimbate în baza prezentului Acord vor fi:

   a. pentru România: **SECRET DE SERVICIU (RESTRICTED), SECRET (CONFIDENTIAL), STRICT SECRET (SECRET)** şi **STRICT SECRET DE IMPORTANŢĂ DEOSEBITĂ (TOP SECRET);**

   b. pentru Regatul Norvegiei: **BEGRENSET (RESTRICTED), KONFIDENSIELT (CONFIDENTIAL), HEMMELIG (SECRET)** şi **STRENGT HEMMELIG (TOP SECRET).**

2. Părţile au stabilit următoarele echivalenţe ale Clasificărilor de Securitate naţionale:

România	Regatul Norvegiei	Echivalentul în limba engleză
STRICT SECRET DE IMPORTANŢĂ DEOSEBITĂ	STRENGT HEMMELIG	TOP SECRET
STRICT SECRET	HEMMELIG	SECRET
SECRET	KONFIDENSIELT	CONFIDENTIAL
SECRET DE SERVICIU	BEGRENSET	RESTRICTED

ARTICOLUL 5
CERTIFICATELE DE SECURITATE A PERSONALULUI

1. Fiecare Parte va garanta că orice persoană care, prin natura serviciului sau a funcției, necesită acces la Informații Clasificate ale celeilalte Părți, deține Certificat de Securitate a Personalului valabil și corespunzător Clasificării de Securitate, emis de Autoritatea Competentă de Securitate sau de alte autorități corespunzător desemnate în conformitate cu legislația națională respectivă.

2. Certificatul de Securitate a Personalului va fi emis după efectuarea verificării de securitate în conformitate cu legislația națională a fiecărei Părți, și va corespunde nivelului necesar pentru acces la Informații Clasificate naționale cu Clasificare de Securitate echivalentă.

3. La cerere, Autoritățile Competente de Securitate / Autoritățile Desemnate de Securitate ale statelor Părților își pot acorda reciproc asistență în efectuarea verificării de securitate pentru emiterea Certificatelor de Securitate a Personalului și a Certificatelor de Securitate Industrială / Autorizațiilor de Securitate Industrială, în conformitate cu legislațiile lor naționale.

4. Părțile își vor recunoaște reciproc Certificatele de Securitate a Personalului și Certificatele de Securitate Industrială / Autorizațiile de Securitate Industrială emise conform legislațiilor naționale, în ceea ce privește accesul la Informațiile Clasificate schimbate în baza prezentului Acord.

ARTICOLUL 6
TRANSMITEREA INFORMAȚIILOR CLASIFICATE

1. Transmiterea Informațiilor Clasificate către Terți se poate realiza numai cu acordul prealabil scris al Autorității Competente de Securitate a Părții emitente, care poate impune restricții suplimentare în ceea ce privește transmiterea.

2. Fiecare Parte va lua măsuri ca Informațiile Clasificate primite de la cealaltă Parte să fie utilizate numai în scopul pentru care au fost transmise.

3. Prezentul Acord nu va fi invocat de nici una dintre Părți în scopul obținerii de Informații Clasificate pe care cealaltă Parte le-a primit de la un Terț.

ARTICOLUL 7
AUTORITĂȚILE COMPETENTE DE SECURITATE

1. Autoritățile Competente de Securitate responsabile, la nivel național, de implementarea şi de controlul măsurilor întreprinse pentru implementarea prezentului Acord sunt:

În România	În Regatul Norvegiei
Guvernul României Oficiul Registrului Național al Informațiilor Secrete de Stat București – Str. Mureş nr.4 sector 1 ROMÂNIA	Nasjonal sikkerhetsmyndighet Postboks 14 1306 Bærum postterminal NORWAY

2. În vederea aplicării aceloraşi standarde de securitate, fiecare Autoritate Competentă de Securitate va furniza, la cerere, celeilalte Autorități Competente de Securitate informații referitoare la organizarea şi procedurile ei de securitate. În acest sens, Autoritățile Competente de Securitate pot conveni asupra efectuării de vizite reciproce de către funcționari autorizați, în ambele țări.

ARTICOLUL 8
VIZITELE

1. Vizitele ce implică acces la Informații Clasificate sau în incinte unde sunt emise, gestionate sau depozitate Informații Clasificate, sau în care se desfăşoară activități ce implică Informații Clasificate, vor fi permise de către o Parte vizitatorilor din statul celeilalte Părți dacă s-a obținut permisiunea prealabilă scrisă din partea Autorității Competente de Securitate / Autorității Desemnate de Securitate a Părții primitoare. O astfel de permisiune se va acorda numai persoanelor care dețin Certificate de Securitate a Personalului corespunzătoare, în conformitate cu principiul Necesității de a cunoaşte.

2. Vizitele vor fi anunțate, de regulă, cu douăzeci (20) de zile lucrătoare înainte.

3. În cazuri urgente, cererea de vizită poate fi transmisă mai devreme, dar nu cu mai puțin de cinci (5) zile lucrătoare înainte.

4. Cererea de vizită va cuprinde:

a. Numele şi prenumele vizitatorului, locul şi data naşterii, cetăţenia, angajatorul, seria paşaportului sau a altor documente de identitate ale vizitatorului;
b. Confirmarea Certificatului de Securitate a Personalului în concordanţă cu scopul vizitei;
c. Menţionarea detaliată a scopului vizitei sau vizitelor;
d. Data şi durata preconizate pentru efectuarea vizitei sau vizitelor solicitate;
e. Persoana de contact de la locaţiile ce urmează a fi vizitate, contactele anterioare şi orice alte informaţii utile pentru a se stabili oportunitatea vizitei sau vizitelor.

5. Valabilitatea autorizaţiilor de vizită nu va depăşi douăsprezece (12) luni.

6. Fiecare Parte va asigura protecţia datelor personale ale vizitatorilor conform legislaţiei sale naţionale.

ARTICOLUL 9
SECURITATEA INDUSTRIALĂ

1. În cazul în care o Parte sau o persoană juridică din statul său intenţionează să încredinţeze un Contract Clasificat ce urmează a se derula pe teritoriul statului celeilalte Părţi, Partea din statul în care se derulează contractul îşi va asuma responsabilitatea de a proteja Informaţiile Clasificate legate de contract, în conformitate cu legislaţia naţională proprie.

2. Anterior transmiterii către Contractori sau Sub-Contractori ori potenţiali Contractori sau Sub-Contractori a oricăror Informaţii Clasificate primite de la cealaltă Parte, Partea primitoare, prin intermediul Autorităţii Competente de Securitate:

a. va emite Certificat de Securitate Industrială / Autorizaţie de Securitate Industrială de nivel corespunzător pentru Contractori sau Sub-Contractori ori potenţiali Contractori sau Sub-Contractori, cu condiţia ca aceştia să îndeplinească cerinţele necesare eliberării acestuia/acesteia;

b. va confirma că toate persoanele ale căror îndatoriri presupun acces la Informaţii Clasificate deţin Certificate de Securitate a Personalului de nivel corespunzător.

3. Părţile vor lua măsuri ca fiecare Contract Clasificat să cuprindă o Anexă de Securitate corespunzătoare care să conţină o Listă a Clasificărilor de Securitate.

4. Procedurile mai detaliate referitoare la activitățile industriale care implică Informații Clasificate pot fi elaborate și convenite între Autoritățile Competente de Securitate ale statelor Părților.

5. Părțile vor asigura protecția drepturilor de autor, drepturilor de proprietate industrială – inclusiv patentele – și a oricăror altor drepturi legate de Informațiile Clasificate schimbate între statele lor, în conformitate cu legislațiile lor naționale.

ARTICOLUL 10
TRANSMITEREA INFORMAȚIILOR CLASIFICATE

1. Informațiile Clasificate vor fi transmise, de regulă, prin curier diplomatic sau militar. Partea primitoare va confirma primirea Informațiilor Clasificate.

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

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

4. Schimbul de Informații Clasificate prin intermediul sistemelor informatice și de comunicații se va efectua conform procedurilor de securitate stabilite prin aranjamente reciproce convenite de către ambele Autorități Competente de Securitate.

ARTICOLUL 11
INCIDENTELE DE SECURITATE ȘI COMPROMITEREA INFORMAȚIILOR CLASIFICATE

1. În cazul producerii unui Incident de Securitate care duce la Compromiterea sau posibila Compromitere a Informațiilor Clasificate, Autoritatea Competentă de Securitate din statul pe teritoriul căruia s-a produs Incidentul de Securitate va informa imediat Autoritatea Competentă de Securitate a celeilalte Părți, va asigura investigația de securitate adecvată a acestei situații și va lua măsurile necesare de limitare a consecințelor, în conformitate cu legislația sa națională. Dacă va fi necesar, Autoritățile Competente de Securitate vor coopera la investigație.

2. În cazul în care compromiterea se produce pe teritoriul unui stat terț, Autoritatea Competentă de Securitate din statul Părții care a transmis informațiile, va acționa conform alineatului 1.

3. După încheierea investigațiilor, Autoritatea Competentă de Securitate / Autoritatea Desemnată de Securitate din statul pe teritoriul căruia a avut loc compromiterea sau posibila Compromitere a Informațiilor Clasificate va comunica imediat, în scris, Autorității Competente de Securitate din statul celeilalte Părți rezultatele și concluziile investigației.

ARTICOLUL 12
SOLUȚIONAREA DIFERENDELOR

Orice diferend privind interpretarea sau implementarea prezentului Acord se va soluționa prin consultări între Părți și nu va fi deferit unui tribunal național sau internațional ori unui Terț.

ARTICOLUL 13
CHELTUIELI

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

ARTICOLUL 14
ASISTENȚA RECIPROCĂ

1. Părțile se pot consulta reciproc cu privire la implementarea și interpretarea prevederilor prezentului Acord.

2. Dacă este nevoie, Autoritățile Competente de Securitate din statele Părților se vor consulta reciproc în legătură cu aspecte tehnice specifice privind implementarea prezentului Acord și pot conveni asupra încheierii unor protocoale de securitate speciale, adiționale la prezentul Acord, de la caz la caz.

ARTICOLUL 15
RAPORTURI CU ACORDURI EXISTENTE

1. După intrarea în vigoare a prezentului Acord, Informațiile Clasificate schimbate în baza Acordului bilateral de securitate dintre Ministerul Apărării Naționale din România şi Ministerul Apărării din Regatul Norvegiei, semnat la Bucureşti la 9 noiembrie 2000 şi la Oslo la 15 ianuarie 2001, vor fi protejate conform prevederilor prezentului Acord.

2. Prevederile paragrafului 1 se vor aplica şi pentru protecția Informațiilor Clasificate schimbate în baza altor aranjamente, încheiate anterior între Părți.

3. La data intrării în vigoare a prezentului Acord, Acordul bilateral de securitate dintre Ministerul Apărării Naționale din România şi Ministerul Apărării din Regatul Norvegiei, semnat la Bucureşti la 9 noiembrie 2000 şi la Oslo la 15 ianuarie 2001, îşi va înceta valabilitatea.

ARTICOLUL 16
DISPOZIȚII FINALE

1. Prezentul Acord este încheiat pe perioadă nedeterminată şi urmează a fi supus aprobării în conformitate cu procedurile naționale ale statului fiecărei Părți.

2. Prezentul Acord intră în vigoare în prima zi a celei de-a doua luni de la data ultimei notificări, pe căi diplomatice, privind îndeplinirea de către Părți a procedurilor lor interne necesare intrării în vigoare a acestuia.

3. Fiecare Parte are dreptul să denunțe oricând prezentul Acord. În acest caz, valabilitatea Acordului expiră după 6 (şase) luni de la data la care notificarea de denunțare a fost transmisă pe căi diplomatice celeilalte Părți.
Chiar şi în situația denunțării prezentului Acord, toate Informațiile Clasificate furnizate în baza prezentului Acord vor continua să fie protejate în conformitate cu prevederile acestuia.

4. Prezentul Acord poate fi amendat prin consimțământul reciproc al Părților. Amendamentele vor intra în vigoare în conformitate cu prevederile alineatului 1 al prezentului articol.

5. Fiecare Parte va notifica cu promptitudine celeilalte Părți orice modificări survenite în legislația sa națională care ar putea afecta protecția Informațiilor Clasificate în conformitate cu prezentul Acord. Într-o asemenea situație,

Părțile se vor consulta în legătură cu oportunitatea unor modificări ale prezentului Acord. Între timp, Informațiile Clasificate vor continua să fie protejate aşa cum s-a stabilit în prezentul Acord, dacă Partea emitentă nu solicită altfel, în scris.

Semnat la Bucureşti la 29 mai 2008 în două exemplare originale, fiecare în limbile română, norvegiană şi engleză, toate textele fiind egal valabile. În caz de divergențe de interpretare, va prevala textul în limba engleză.

Pentru
Guvernul României

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

Pentru
Guvernul Regatului Norvegiei

ØYSTEIN HOVDKINN
Ambasadorul Regatului Norvegiei

conform cu originalul

SIKKERHETSAVTALE

MELLOM

ROMANIAS REGJERING

OG

KONGERIKET NORGES REGJERING

OM GJENSIDIG BESKYTTELSE AV GRADERT INFORMASJON

Romanias regjering og Kongeriket Norges regjering,

heretter kalt partene,

har, for å trygge gradert informasjon utvekslet direkte eller via rettssubjekter som befatter seg med gradert informasjon tilhørende motpartens stat, og innenfor rammen av de aktiviteter som faller inn under partenes kompetanse,

inngått følgende avtale:

ARTIKKEL 1
VIRKEOMRÅDE

1. Formålet med denne avtale er å sørge for beskyttelse av gradert informasjon som utveksles eller blir til som et ledd i samarbeidet mellom partene.

2. Beslutningen om å overføre eller utveksle gradert informasjon skal fattes i samsvar med partenes nasjonale lovgivning.

3. Denne avtale skal regulere enhver aktivitet og være en integrert del av enhver kontrakt eller avtale som innebærer befatning med gradert informasjon og som inngås mellom partene eller rettssubjekter i partsstatene.

4. Denne avtale skal ikke påvirke partenes forpliktelser etter andre internasjonale avtaler, og skal ikke brukes mot andre staters interesser, sikkerhet eller territoriale integritet.

ARTIKKEL 2
DEFINISJONER

I forbindelse med denne avtale gjelder at:

a. **gradert informasjon** betyr:
informasjon, dokument eller materiale, uansett i hvilken fysisk form, som er tildelt en sikkerhetsgradering i samsvar med de respektive lands lovgivning og som skal beskyttes tilsvarende,

b. **gradert dokument** betyr:
enhver form for nedtegnelse som inneholder gradert informasjon uansett form eller fysiske kjennetegn, herunder uten begrensning skriftstykker eller trykksaker, databehandlingskort og -bånd, kart, sjøkart, fotografier, malerier, tegninger, inngraveringer, skisser, arbeidsnotater og arbeidspapirer, gjennomslag og fargebånd, reproduksjoner uansett etter hvilken metode og prosess de er framstilt, samt lyd- og stemmeopptak, magnetiske eller optiske nedtegnelser eller videoopptak i enhver form, og bærbart automatisert databehandlingsutstyr med residente datalagringsmedier samt uttakbare datalagringsmedier,

c. **gradert materiale** betyr:
gjenstand eller del av maskineri, prototyp, utstyr, våpen osv., håndlagd eller mekanisk framstilt, som er produsert eller er under produksjon og som er tildelt en sikkerhetsgradering,

d. **sikkerhetsgradering** betyr:
tilordning til et graderingsnivå eller en graderingsklasse i samsvar med partenes nasjonale lovgivning,

e. **gradert kontrakt** betyr:
avtale mellom to eller flere kontrahenter som etablerer og definerer deres rettigheter og forpliktelser, og som inneholder eller innebærer befatning med gradert informasjon,

f. **kontrahent eller underleverandør** betyr:
person eller rettssubjekt med rettsevne til å inngå graderte kontrakter,

g. **sikkerhetsbrudd** betyr:
en handling eller unnlatelse i strid med partenes nasjonale lovgivning som resulterer i en faktisk eller potensiell kompromittering av gradert informasjon,

h. **kompromittering av gradert informasjon** betyr:
en situasjon der gradert informasjon – som følge av sikkerhetsbrudd eller fiendtlig aktivitet (f.eks. spionasje, terrorhandling eller tyveri) – ikke lenger er fortrolig, intakt eller tilgjengelig, eller der understøttende tjenester og ressurser ikke lenger er intakt eller tilgjengelige. Dette omfatter tap, delvis eller fullstendig avsløring, ulovlig modifisering og ødeleggelse eller tjenestenektelse,

i. **sikkerhetsspesifikasjonsbrev** betyr:
et dokument utstedt av vedkommende myndighet som del av en gradert kontrakt eller underkontrakt som fastsetter sikkerhetskravene eller de deler av kontrakten som krever sikkerhetsbeskyttelse,

j. **graderingssjekkliste** betyr:
en liste over gradert informasjon, materiale og virksomhet tilknyttet en gradert kontrakt og deres sikkerhetsgradering, som inngår i sikkerhetsspesifikasjonsbrevet,

k. **personellklareringsbevis** betyr:
et dokument som bekrefter at innehaveren i utførelsen av sine oppgaver kan gis tilgang til gradert informasjon med en bestemt sikkerhetsgradering på grunnlag av prinsippet om behov for innsyn, utstedt i overensstemmelse med partenes nasjonale lovgivning,

l. **leverandørklareringsbevis / industrisikkerhetsautorisasjon** betyr:
et dokument som bekrefter at et rettssubjekt har godkjennelse til å utføre industrivirksomhet som krever tilgang til gradert informasjon, utstedt i overensstemmelse med partenes nasjonale lovgivning,

m. **behov for innsyn** betyr:
det prinsipp at tilgang til gradert informasjon bare kan innvilges individuelt for personer som i utførelsen av sine oppgaver har behov for å arbeide med eller å ha tilgang til slik informasjon,

n. **kompetent sikkerhetsmyndighet** betyr:
en institusjon utstyrt med fullmakter på nasjonalt plan som i samsvar med partenes nasjonale lovgivning sørger for enhetlig gjennomføring av beskyttelsestiltakene for gradert informasjon. Disse myndighetene er oppført i artikkel 7 i denne avtale,

o. **utpekt sikkerhetsmyndighet** betyr:
den institusjon som, i overensstemmelse de respektive parters nasjonale lovgivning, er bemyndiget på sitt aktivitets- og ansvarsområde til å etablere sine egne strukturer og tiltak med henblikk på å koordinere og kontrollere den virksomhet som gjelder beskyttelse av gradert informasjon. På området beskyttelse av gradert informasjon står utpekt sikkerhetsmyndighet under ledelse av kompetent sikkerhetsmyndighet,

p. **tredjepart** betyr:
stat, enkeltperson, nasjonal eller internasjonal organisasjon, privat eller offentlig enhet som ikke er part i denne avtale.

ARTIKKEL 3
BESKYTTELSE AV GRADERT INFORMASJON

1. I samsvar med nasjonal lovgivning skal partene treffe egnede tiltak for å beskytte gradert informasjon som overføres, mottas, frambringes eller utvikles som et resultat av enhver avtale eller forbindelse mellom partene eller mellom rettssubjekter i partsstatene. All gradert informasjon som utveksles, mottas, frambringes eller utvikles, skal av partene gis samme graderingsnivå som partene gir sin egen graderte informasjon av tilsvarende art, som definert i artikkel 4 i denne avtale.

2. Den mottakende part skal verken benytte et lavere graderingsnivå for mottatt gradert informasjon eller nedgradere informasjonen uten skriftlig forhåndssamtykke fra den kompetente myndighet hos den utstedende part. Den kompetente sikkerhetsmyndighet hos den utstedende part skal informere den kompetente sikkerhetsmyndighet hos mottakerparten om eventuelle endringer i sikkerhetsgradering for utvekslet informasjon.

3. Reproduksjon eller modifikasjon av mottatt gradert informasjon kan foretas med mindre annet er uttrykkelig bestemt av den utstedende part. Reproduksjoner av gradert informasjon skal utstyres med graderingsnivåer tilsvarende sikkerhetsgraderingen av originalen, og skal beskyttes på samme måte som originalinformasjonen.
Antall kopier skal være begrenset til det som er påkrevd til offisielle formål. Informasjon gradert STRICT SECRET DE IMPORTANȚĂ DEOSEBITĂ / STRENGT HEMMELIG / TOP SECRET skal bare reproduseres etter skriftlig forhåndssamtykke fra den utstedende part.

4. Gradert informasjon og materiale må bare tilintetgjøres etter skriftlig forhåndssamtykke fra eller på anmodning av den utstedende part, i samsvar med partenes nasjonale lovgivning og på en slik måte at fullstendig eller delvis rekonstruksjon av gradert informasjon er umulig. Dersom den utstedende part ikke samtykker i at gradert informasjon tilintetgjøres, skal det graderte materialet eller dokumentet returneres til den. Informasjon merket STRICT SECRET DE IMPORTANȚĂ DEOSEBITĂ / STRENGT HEMMELIG / TOP SECRET skal ikke tilintetgjøres, men returneres til den utstedende part.

Ved overhengende fare skal gradert informasjon tilintetgjøres uten tillatelse på forhånd. Den utstedende parts kompetente sikkerhetsmyndighet skal omgående underrettes om dette.

5. Den mottakende part skal underrette den utstedende part om at gradert informasjon er tilintetgjort.

6. Tilgang til gradert informasjon og/eller til lokaliteter og anlegg der det foregår aktiviteter som innebærer befatning med gradert informasjon, eller der gradert informasjon oppbevares, forutsetter at prinsippet om behov for innsyn er innfridd, og skal bare innvilges for personer med gyldig personellklareringsbevis på det graderingsnivå som gjelder for informasjonen som det anmodes om tilgang til.

7. Hver part skal, blant annet gjennom kontrollbesøk, påse at de rettssubjekter som innehar, utvikler, frambringer og/eller bruker gradert informasjon tilhørende motpartens stat, overholder partenes nasjonale lovgivning.

8. Før en representant for en part utleverer gradert informasjon til en representant for den annen part, skal den mottakende part underrette den utstedende part om at førstnevnte representant har personellklareringsbevis på høyeste graderingsnivå for den informasjon vedkommende skal ha tilgang til, og at den graderte informasjonen er beskyttet i samsvar med bestemmelsene i denne avtale.

ARTIKKEL 4
SIKKERHETSGRADERINGER

1. Sikkerhetsgraderingene som gjelder for informasjon som utveksles innenfor rammen av denne avtale, skal være:

a. for Romania: **SECRET DE SERVICIU (RESTRICTED), SECRET (CONFIDENTIAL), STRICT SECRET (SECRET)** og **STRICT SECRET DE IMPORTANȚĂ DEOSEBITĂ (TOP SECRET);**

b. for Kongeriket Norge: **BEGRENSET (RESTRICTED), KONFIDENSIELT (CONFIDENTIAL), HEMMELIG (SECRET)** og **STRENGT HEMMELIG (TOP SECRET).**

2. Partene har bestemt at samsvaret mellom de nasjonale sikkerhetsgraderingene er som følger:

Romania	Kongeriket Norge	Engelsk motstykke
STRICT SECRET DE IMPORTANȚĂ DEOSEBITĂ	STRENGT HEMMELIG	TOP SECRET
STRICT SECRET	HEMMELIG	SECRET
SECRET	KONFIDENSIELT	CONFIDENTIAL
SECRET DE SERVICIU	BEGRENSET	RESTRICTED

ARTIKKEL 5
PERSONELLKLARERINGSBEVIS

1. Hver part skal garantere at enhver person som på grunn av sin stilling eller sine oppgaver trenger tilgang til gradert informasjon tilhørende motparten, har gyldig personellklareringsbevis tilsvarende det aktuelle graderingsnivå, utstedt av den kompetente sikkerhetsmyndighet eller av andre myndigheter som er behørig utpekt i samsvar med vedkommende nasjonale lovgivning.

2. Personellklareringsbevis skal utstedes etter gjennomført sikkerhetsundersøkelse i samsvar med hver parts nasjonale lovgivning, og skal tilsvare det nivå som kreves for tilgang til nasjonal gradert informasjon med motsvarende sikkerhetsgradering.

3. På anmodning kan partsstatenes kompetente sikkerhetsmyndigheter / utpekte sikkerhetsmyndigheter bistå hverandre, hver i samsvar med sin nasjonale lovgivning, i undersøkelsene med henblikk på utstedelse av personellklareringsbevis og leverandørklareringsbevis / industrisikkerhetsautorisasjon.

4. Hva angår tilgang til gradert informasjon utvekslet i henhold til denne avtale, skal partene gjensidig anerkjenne de personellklareringsbevis og leverandørklareringsbevis / industrisikkerhetsautorisasjoner som utstedes i samsvar med deres nasjonale lovgivning.

ARTIKKEL 6
FRIGIVELSE AV GRADERT INFORMASJON

1. Frigivelse av gradert informasjon til tredjeparter må bare skje etter skriftlig forhåndssamtykke fra den utstedende parts kompetente sikkerhetsmyndighet, som kan legge ytterligere begrensninger på frigivelsen.

2. Hver part skal sikre at gradert informasjon som mottas fra motparten, bare brukes til det formål som lå til grunn for at informasjonen ble frigitt.

3. Ingen av partene skal påberope seg denne avtale for å tilegne seg gradert informasjon som motparten har mottatt fra en tredjepart.

ARTIKKEL 7
KOMPETENTE SIKKERHETSMYNDIGHETER

1. De kompetente sikkerhetsmyndigheter som er ansvarlige på nasjonalt plan for gjennomføringen av og kontrollen med de tiltak som iverksettes i forbindelse med gjennomføringen av denne avtale, er:

I Romania	I Kongeriket Norge
Guvernul României Oficiul Registrului Național al Informațiilor Secrete de Stat București - Str. Mureș nr. 4 sector 1 ROMÂNIA	Nasjonal sikkerhetsmyndighet Postboks 14 1306 Bærum postterminal NORWAY

2. For å opprettholde samme sikkerhetsstandard skal hver kompetent sikkerhetsmyndighet etter anmodning gi den annen kompetente sikkerhetsmyndighet opplysninger om egen sikkerhetsorganisering og egne sikkerhetsprosedyrer. Med henblikk på dette kan de kompetente sikkerhetsmyndigheter også avtale gjensidige besøk i begge land ved godkjente tjenestemenn.

ARTIKKEL 8
BESØK

1. Besøk som forutsetter tilgang til gradert informasjon eller til steder der slik informasjon skapes, håndteres eller oppbevares, eller der aktiviteter som innebærer befatning med gradert informasjon foregår, skal bare innvilges av den ene part for besøkende fra motpartens stat etter at det på forhånd er innhentet skriftlig tillatelse fra den mottakende parts kompetente sikkerhetsmyndighet / utpekte sikkerhetsmyndighet. Slik tillatelse skal bare gis til personer som innehar nødvendig personellklareringsbevis og har behov for innsyn.

2. Besøk skal normalt varsles tjue (20) virkedager i forveien.

3. I presserende tilfeller kan fristen for anmodning om besøk gjøres kortere, men ikke kortere enn fem (5) virkedager før besøket.

4. En besøksanmodning skal inneholde:
a. en besøkendes etternavn, fornavn, fødested og fødselsdato, statsborgerskap, arbeidsgiver, pass eller annet identitetsdokument,
b. bekreftelse på den besøkendes personellklareringsbevis i samsvar med besøkets formål,
c. detaljert angivelse av besøkets eller besøkenes formål,
d. besøkets eller besøkenes forventede dato og varighet,
e. kontaktperson på stedet som skal besøkes, tidligere kontakter og eventuell annen informasjon som kan bidra til å bekrefte at besøket eller besøkene er velbegrunnet.

5. Besøksgodkjennelser skal ikke være gyldige i mer enn tolv (12) måneder.

6. Hver part skal garantere beskyttelse av besøkendes personopplysninger i samsvar med egen nasjonal lovgivning.

ARTIKKEL 9
INDUSTRISIKKERHET

1. Dersom en part eller et rettssubjekt i dens stat akter å tildele en gradert kontrakt for utførelse på motpartens statsterritorium, skal parten i hvis stat

utførelsen skjer, påta seg ansvaret for å beskytte gradert informasjon tilknyttet kontrakten i samsvar med sin nasjonale lovgivning.

2. Før gradert informasjon som mottas fra motparten, frigis til kontrahenter/underleverandører eller til potensielle kontrahenter/underleverandører, skal den mottakende part via den kompetente sikkerhetsmyndighet:

a. utstede leverandørklareringsbevis/industrisikkerhetsautorisasjon på tilstrekkelig nivå til kontrahentene/underleverandørene eller til potensielle kontrahenter/underleverandører, forutsatt at de har oppfylt kravene til slik utstedelse,

b. bekrefte at alt personell hvis oppgaver krever tilgang til gradert informasjon, innehar personellklareringsbevis på tilstrekkelig nivå.

3. Partene skal påse at hver gradert kontrakt omfatter et passende sikkerhetsspesifikasjonsbrev som inneholder en sjekkliste for sikkerhetsgradering.

4. Mer detaljerte prosedyrer i tilknytning til industrivirksomhet som omfatter gradert informasjon, kan utarbeides og avtales mellom partsstatenes kompetente sikkerhetsmyndigheter.

5. Partene skal sikre beskyttelse av opphavsrett, industriell eiendomsrett – herunder patenter – og eventuelle andre rettigheter i tilknytning til den graderte informasjon som utveksles mellom deres stater, i samsvar med deres nasjonale lovgivning.

ARTIKKEL 10
OVERFØRING AV GRADERT INFORMASJON

1. Gradert informasjon skal normalt overleveres av diplomatisk eller militær kurér. Den mottakende part skal bekrefte mottakelsen av gradert informasjon.

2. Dersom en stor forsendelse inneholdende gradert informasjon skal overføres, skal de kompetente sikkerhetsmyndigheter gjensidig avtale og godkjenne transportmidlene, rutene og sikkerhetstiltakene for hvert slikt tilfelle.

3. Andre godkjente overførings- eller utvekslingsmetoder for gradert informasjon kan benyttes dersom begge kompetente sikkerhetsmyndigheter er enige om det.

4. Utveksling av gradert informasjon via informasjons- og kommunikasjonssystemer skal skje i samsvar med de sikkerhetsprosedyrer som er etablert gjennom gjensidige ordninger som de to kompetente sikkerhetsmyndigheter har avtalt.

ARTIKKEL 11
SIKKERHETSBRUDD OG KOMPROMITTERING AV GRADERT INFORMASJON

1. Ved sikkerhetsbrudd som resulterer i kompromittering eller mulig kompromittering av gradert informasjon, skal den kompetente sikkerhetsmyndighet i staten der sikkerhetsbruddet fant sted, omgående informere den kompetente sikkerhetsmyndighet i motpartens stat og i samsvar med sin nasjonale lovgivning sørge for grundig sikkerhetsetterforskning av hendelsen og for nødvendige tiltak for å begrense følgene. Om nødvendig skal de kompetente sikkerhetsmyndigheter samarbeide om etterforskningen.

2. Dersom kompromitteringen finner sted i en tredjestat, skal den kompetente sikkerhetsmyndighet i avsenderstaten treffe tiltak som nevnt i nr. 1.

3. Når etterforskningen er fullført, skal den kompetente sikkerhetsmyndighet / den utpekte sikkerhetsmyndighet i staten der kompromitteringen eller den potensielle kompromitteringen av gradert informasjon fant sted, omgående informere den kompetente sikkerhetsmyndighet i motpartens stat skriftlig om resultatene av slik etterforskning.

ARTIKKEL 12
TVISTELØSNING

Tvister om tolkningen eller anvendelsen av denne avtale skal løses ved konsultasjoner mellom partene, og skal ikke bringes inn for noen nasjonal eller internasjonal domstol eller tredjepart for avgjørelse.

ARTIKKEL 13
OMKOSTNINGER

Hver part skal dekke sine egne omkostninger i forbindelse med gjennomføringen av denne avtale.

ARTIKKEL 14
GJENSIDIG BISTAND

1. Partene kan konsulterer hverandre om anvendelsen og tolkningen av bestemmelsene i denne avtale.

2. Skulle behovet oppstå, vil partsstatenes kompetente sikkerhetsmyndigheter konsultere hverandre om konkrete tekniske aspekter ved gjennomføringen av denne avtale, og kan gjensidig slutte seg til at det vedtas ytterligere sikkerhetsprotokoller av spesifikk art til denne avtale fra sak til sak.

ARTIKKEL 15
FORHOLD TIL EKSISTERENDE AVTALER

1. Etter at denne avtale har trådt i kraft, skal gradert informasjon som er utvekslet på grunnlag av Bilateral sikkerhetsavtale mellom Romanias nasjonale forsvarsministerium og Kongeriket Norges forsvarsdepartement, undertegnet i Bucuresti 9.11.2000 og Oslo 15.1.2001, beskyttes i henhold til bestemmelsene i denne avtale.

2. Bestemmelsene i nr. 1 skal også gjelde for beskyttelse av gradert informasjon som er utvekslet på grunnlag av andre avtaler som tidligere er inngått mellom partene.

3. Når denne avtale trer i kraft, opphører Bilateral sikkerhetsavtale mellom Romanias nasjonale forsvarsministerium og Kongeriket Norges forsvarsdepartement, undertegnet i Bucuresti 9.11.2000 og Oslo 15.1.2001.

ARTIKKEL 16
SLUTTBESTEMMELSER

1. Denne avtale inngås på ubestemt tid og må godkjennes i samsvar med de nasjonale prosedyrer i hver partsstat.

2. Denne avtale trer i kraft første dag i annen måned etter mottakelsen av den siste underretningen partene imellom om at de nødvendige krav for at denne avtale skal tre i kraft er oppfylt.

3. Hver part kan når som helst si opp denne avtale. Avtalens gyldighet opphører da 6 (seks) måneder etter datoen da underretningen med varsel om oppsigelse er forkynt for motparten. Selv om denne avtale sies opp, skal all gradert informasjon som er utlevert i henhold til avtalen, fortsatt beskyttes i samsvar med bestemmelsene her.

4. Denne avtale kan endres etter samtykke fra begge parter. Slike endringer trer i kraft i samsvar med bestemmelsene i nr. 1 i denne artikkel.

5. Hver part skal omgående underrette den annen part om eventuelle endringer i sin nasjonale lovgivning som vil påvirke beskyttelsen av gradert informasjon i henhold til denne avtale. I slike tilfeller skal partene konsultere hverandre for å vurdere mulige endringer i denne avtale. I mellomtiden skal gradert informasjon fortsatt beskyttes som beskrevet her, med mindre den utstedende part skriftlig anmoder om noe annet.

Undertegnet i Bucuresti den 29. mai 2008 i to originaleksemplarer, hvert på rumensk, norsk og engelsk, hvorav alle tekster har samme gyldighet. Ved avvikende tolkning har engelsk tekst forrang.

For Romanias regjering

MARIUS PETRESCU
statssekretær
direktør
Nasjonalt arkiv for gradert informasjon

For Kongeriket Norges regjering

ØYSTEIN HOVDKINN
Norges ambassadør

SECURITY AGREEMENT

BETWEEN

THE GOVERNMENT OF ROMANIA

AND

THE GOVERNMENT OF THE KINGDOM OF NORWAY

ON MUTUAL PROTECTION OF CLASSIFIED INFORMATION

The Government of Romania and the Government of the Kingdom of Norway, hereafter called the Parties,

In order to safeguard the Classified Information exchanged directly or through legal entities which deal with Classified Information of the state of the other Party and within the framework of activities which fall under the competencies of the Parties,

Have agreed on the following:

ARTICLE 1
APPLICABILITY

1. The objective of this Agreement is to ensure the protection of Classified Information that is exchanged or created in the process of co-operation between the Parties.

2. The decision of transfer or exchange of Classified Information shall be adopted in accordance with the national legislations of the Parties.

3. This Agreement shall govern any activities, and form an integral part of any contract or agreement involving Classified Information, concluded between the Parties or legal entities of the states of the Parties.

4. This Agreement shall not affect the commitments of both Parties which stem from other international agreements and shall not be used against the interests, security and territorial integrity of other states.

ARTICLE 2
DEFINITIONS

For the purpose of this Agreement:

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

b. **Classified Document** means:
any sort of record containing Classified Information regardless of its form or physical characteristic, including, without limitation, written or printed matters, data processing cards and tapes, maps, charts, photographs, paintings, drawings, engravings, sketches, working notes and papers, carbon copies and ink ribbons, or reproductions produced by any means or processes, and sound, voice, magnetic 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 etc., 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 national legislations of the Parties;

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

f. **Contractor or Sub-Contractor** means:
an individual or legal entity possessing the legal capability to conclude Classified Contracts;

g. **Breach of Security** means:
an act or omission contrary to the national legislations 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 (such as espionage, act of terrorism or theft) – Classified Information has lost its confidentiality, integrity or availability, or when supporting services and resources have lost their integrity or availability. This includes 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 Classifications, included in the Security Aspects Letter;

k. **Personnel Security Clearance Certificate** means:
a document certifying that, in performing his/her duties, the holder may have access to Classified Information of a certain Security Classification, in compliance with the Need-to-Know principle, issued in accordance with the national legislations of the Parties;

l. **Facility Security Clearance Certificate / Industrial Security Authorization** means:
a document certifying that a legal entity is authorized to carry out industrial activities requiring access to Classified Information, issued in accordance with the national legislations of the Parties;

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:
an institution empowered with authority at national level which, in compliance with the national legislations of the Parties, ensures the unitary implementation of the protective measures for Classified Information. Such authorities are listed in Article 7 of this Agreement;

o. **Designated Security Authority** means:
the institution which, in compliance with the respective national legislation of the Parties, is empowered to establish, for its activity and responsibility field, its own structures and measures regarding the coordination and control of the activity referring to the protection of Classified Information. The Designated Security Authority is coordinated, in the field of the protection of Classified Information, by the Competent Security Authority;

p. **Third Party** means:
any state, individual, institution, national or international organization, private or public entity which is not part to this Agreement.

ARTICLE 3
PROTECTION OF CLASSIFIED INFORMATION

1. In accordance with their national legislations, the Parties shall take appropriate measures to protect Classified Information which is transmitted, received, produced or developed as a result of any agreement or relation between the Parties or legal entities of the states of the Parties. The Parties shall afford to all the exchanged, received, produced or developed Classified Information the same degree of security protection as afforded to their own equivalent Classified Information, as defined in Article 4 of this Agreement.

2. The receiving Party shall neither use a lower Security Classification for the received Classified Information nor declassify this information without the prior written consent of the Competent Security Authority of the state of the originating Party. The Competent Security Authority of the originating Party shall inform the Competent Security Authority of the receiving Party of any changes in the Security Classification of the exchanged information.

3. Reproduction or modification of the received Classified Information may be made unless otherwise explicitly provided by the originating Party. Reproductions of the Classified Information shall receive Security Classification markings equivalent to the Security Classification of the original and shall be protected in the same way as the original information. The number of copies shall be limited to that number necessary for official purposes. Information classified STRICT SECRET DE IMPORTANȚĂ DEOSEBITĂ / STRENGT HEMMELIG / TOP SECRET shall only be reproduced after prior written permission from the originating Party.

4. Classified Information and materials may be destroyed only with the written consent or at the request of the originating Party, in accordance with the national legislations of the Parties, in such a manner that any reconstruction of Classified Information in whole or in part is impossible. Should the originating Party not agree on the destruction of some Classified Information, the Classified Material or document shall be returned to it.

The STRICT SECRET DE IMPORTANȚĂ DEOSEBITĂ / STRENGT HEMMELIG / TOP SECRET information shall not be destroyed but returned to the originating Party.

In case of an imminent danger Classified Information shall be destroyed without prior authorization. The Competent Security Authority of the originating Party shall immediately be notified about this.

5. The receiving Party shall notify the destruction of Classified Information to the originating Party.

6. Access to Classified Information and/or locations and facilities where activities involving Classified Information are performed or where Classified Information is stored is allowed, with the observance of the Need-to-Know principle, only to those individuals having a Personnel Security Clearance Certificate valid for the Security Classification of the information for which the access is required.

7. Each Party shall supervise the observance of the national legislations by the legal entities that hold, develop, produce and/or use Classified Information of the state of the other Party, by means of inter alia review visits.

8. Before a representative of a Party provides Classified Information to a representative of the other Party, the receiving Party shall notify the originating Party that the former representative holds a Personnel Security Clearance Certificate of the highest Security Classification for the information to which he/she is to have access, and that the Classified Information is protected in accordance with the provisions of this Agreement.

ARTICLE 4
SECURITY CLASSIFICATIONS

1. The Security Classifications applicable to information exchanged within the framework of this Agreement shall be:

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

   b. for the Kingdom of Norway: **BEGRENSET (RESTRICTED), KONFIDENSIELT (CONFIDENTIAL), HEMMELIG (SECRET) and STRENGT HEMMELIG (TOP SECRET).**

2. The Parties have determined that the equivalence of the national Security Classifications is as follows:

Romania	The Kingdom of Norway	English Language Equivalent
STRICT SECRET DE IMPORTANȚĂ DEOSEBITĂ	STRENGT HEMMELIG	TOP SECRET
STRICT SECRET	HEMMELIG	SECRET
SECRET	KONFIDENSIELT	CONFIDENTIAL
SECRET DE SERVICIU	BEGRENSET	RESTRICTED

ARTICLE 5
PERSONNEL SECURITY CLEARANCE CERTIFICATES

1. Each Party shall guarantee that any individual who, due to his/her employment or functions needs access to Classified Information of the other Party, shall hold a Personnel Security Clearance Certificate valid and corresponding to the appropriate Security Classification, issued by the Competent Security Authority or by other authorities duly designated in accordance with the respective national legislation.

2. The Personnel Security Clearance Certificate shall be issued following the security vetting conducted in accordance with the national legislation of each Party, and shall correspond to the level required for access to national Classified Information of the equivalent Security Classification.

3. On request, the Competent Security Authorities/Designated Security Authorities of the states of the Parties may assist each other, in accordance with the respective national legislations, in the vetting procedures related to the issue of Personnel Security Clearance Certificates and Facility Security Clearance Certificates/Industrial Security Authorizations.

4. The Parties shall mutually recognize the Personnel Security Clearance Certificates and Facility Security Clearance Certificates/Industrial Security Authorizations issued in accordance with the national legislations, as regards access to Classified Information exchanged under this Agreement.

ARTICLE 6
RELEASE OF CLASSIFIED INFORMATION

1. Release of Classified Information to Third Parties can only take place after a prior 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 only for the purpose for which this information has been released.

3. This Agreement shall not be invoked by either Party to obtain Classified Information that the other Party has received from a Third Party.

ARTICLE 7
COMPETENT SECURITY AUTHORITIES

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

In Romania	In the Kingdom of Norway
Guvernul României Oficiul Registrului Național al Informațiilor Secrete de Stat București – Str. Mureş nr.4 sector 1 ROMÂNIA	Nasjonal sikkerhetsmyndighet Postboks 14 1306 Bærum postterminal NORWAY

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 and procedures. To this end, the Competent Security Authorities may also agree on mutual visits in both countries by certified officials.

ARTICLE 8
VISITS

1. Visits involving access to Classified Information or to premises where such information is created, handled or stored, or where activities involving Classified Information are carried out, shall only be granted by one Party to visitors from the state of the other Party if a prior written permission from the

Competent Security Authority / Designated Security Authority of the receiving Party has been obtained. Such permission shall only be granted to persons who hold appropriate Personnel Security Clearance Certificates and have a Need-to-Know.

2. Visits shall normally be notified twenty (20) working days in advance.

3. In urgent cases, the request for visit could be transmitted earlier, but not less than five (5) working days before.

4. A request for visit shall include:
   a. A visitor's surname, name, place and date of birth, nationality, employer, passport or other identity documents of the visitor;
   b. Confirmation of the visitor's Personnel Security Clearance Certificate in accordance with the purpose of the visit;
   c. Detailed specification of the purpose of the visit or visits;
   d. Expected date and duration of the requested visit or visits;
   e. Point of contact at the premises to be visited, previous contacts and any other information useful to determine the justification of the visit or visits.

5. The validity of visit authorizations shall not exceed twelve (12) months.

6. Each Party shall guarantee the protection of personal data of the visitors according to its national legislation.

ARTICLE 9
INDUSTRIAL SECURITY

1. In the event that a Party or a legal entity of its state intends to award a Classified Contract to be performed within the territory of the state of the other Party, then the Party of the state in which the performance is taking place, will assume responsibility for the protection of Classified Information related to the contract in accordance with its own national legislation.

2. Prior to releasing to Contractors / Sub-Contractors or to prospective Contractors / Sub-Contractors any Classified Information received from the other Party, the receiving Party, through the Competent Security Authority, shall:
   a. issue a Facility Security Clearance Certificate/Industrial Security Authorization of an appropriate level to the Contractors/Sub-Contractors or to prospective Contractors / Sub-Contractors, provided they have met the requirements for its issue;
   b. confirm that all personnel whose duties require access to Classified

Information hold Personnel Security Clearance Certificates of an appropriate level.

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

4. More detailed procedures related to industrial activities involving Classified Information may be developed and agreed between the Competent Security Authorities of the states of the Parties.

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

ARTICLE 10
TRANSMISSION OF CLASSIFIED INFORMATION

1. Classified Information shall normally be transmitted by diplomatic or military courier. The receiving Party shall confirm the receipt of 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 the security measures for each such case.

3. Other approved means of transmission or exchange of Classified Information may be used, if agreed on by both Competent Security Authorities.

4. The exchange of Classified Information through information and communications systems shall take place in accordance with the security procedures established through mutual arrangements agreed on by both Competent Security Authorities.

ARTICLE 11
BREACHES OF SECURITY AND COMPROMISE OF CLASSIFIED INFORMATION

1. In case of a Breach of Security that results in a compromise or possible Compromise of Classified Information, the Competent Security Authority of the state where the Breach of Security occurred, shall promptly inform the Competent Security Authority of the state of the other Party, ensure the proper security investigation of such event and the necessary measures to limit the

consequences, in accordance with its national legislation. If required, the Competent Security Authorities shall cooperate in the investigation.

2. In case the compromise occurs in a third state, the Competent Security Authority of the state of the dispatching Party shall take action as of paragraph 1.

3. After completion of the investigation, the Competent Security Authority / Designated Security Authority of the state where the compromise or possible Compromise of Classified Information occurred, shall immediately inform in writing the Competent Security Authority of the state of the other Party on the findings and conclusions of the investigation.

ARTICLE 12
SETTLEMENT OF DISPUTES

Any dispute regarding the interpretation or implementation of this Agreement shall be settled by consultation between the Parties, and will not be referred to any national or international tribunal or Third Party for settlement.

ARTICLE 13
COSTS

Each Party shall bear its own costs related to the implementation of this Agreement.

ARTICLE 14
MUTUAL ASSISTANCE

1. The Parties may consult each other in the implementation and interpretation of the provisions of this Agreement.

2. Should the need arise, the Competent Security Authorities of the states of the Parties will consult each other on specific technical aspects concerning the implementation of this Agreement and can mutually approve the conclusion of supplementary security protocols of specific nature to this Agreement on a case by case basis.

ARTICLE 15
RELATIONS TO EXISTING AGREEMENTS

1. After entering into force of this Agreement, Classified Information which has been exchanged on the basis of the Bilateral Security Agreement between the Ministry of National Defence of Romania and the Ministry of Defence of the Kingdom of Norway, done in Bucharest on 09.11.2000 and in Oslo on 15.01.2001 shall be protected according to the provisions of the present Agreement.

2. The provisions of Paragraph 1 shall also apply to the protection of Classified Information which has been exchanged on the basis of other agreements, previously concluded by the Parties.

3. When this Agreement enters into force the Bilateral Security Agreement between the Ministry of National Defence of Romania and the Ministry of Defence of the Kingdom of Norway, done in Bucharest on 09.11.2000 and in Oslo on 15.01.2001 shall be terminated.

ARTICLE 16
FINAL PROVISIONS

1. This Agreement is concluded for an indefinite period of time and is subject to approval in accordance with the national procedures of the state of each of the Parties.

2. This Agreement shall enter into force on the first day of the second month following the receipt of the last of the notifications between the Parties that the necessary requirements for this Agreement to enter into force have been met.

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

4. This Agreement may be amended on the basis of the mutual consent of the Parties. Such amendments shall enter into force in accordance with the provisions of paragraph 1 of this Article.

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

Signed in Bucharest on May the 29th 2008, in two original copies, each one in the Romanian, Norwegian and English languages, all texts having equal validity. In case of divergence of interpretation, the English text shall prevail.

For the Government of Romania

MARIUS PETRESCU
Secretary of State
Director General
of the National Registry Office for Classified Information

For the Government of the Kingdom of Norway

ØYSTEIN HOVDKINN
Ambassador

Conform cu originalul