ACORD

ÎNTRE

GUVERNUL ROMÂNIEI

ŞI

GUVERNUL REPUBLICII ESTONIA

PRIVIND PROTECŢIA RECIPROCĂ A INFORMAŢIILOR CLASIFICATE

Guvernul României şi Guvernul Republicii Estonia, denumite în continuare Părţi,

În scopul asigurării protecţiei informaţiilor clasificate schimbate direct între Părţi sau alte organisme de stat, persoane juridice de drept public sau privat care gestionează informaţii clasificate ale statului celeilalte Părţi şi în cadrul activităţilor care cad în responsabilitatea Autorităţilor Naţionale de Securitate ale Părţilor,

Au convenit următoarele:

ARTICOLUL 1
DOMENIUL DE APLICARE

(1) Prezentul Acord va sta la baza tuturor activităţilor ce implică, în conformitate cu legile şi regulamentele naţionale, schimbul de informaţii clasificate între Părţi sau alte organisme de stat ori persoane juridice de drept public sau privat privind:

a) cooperarea între Părţi în domeniul apărării naţionale şi în orice alte aspecte referitoare la securitatea naţională;

b) cooperarea, proiectele comune, contractele sau oricare alte raporturi între organismele de stat sau persoanele juridice de drept public sau privat din statele Părţilor în domeniul apărării naţionale şi referitor la oricare alte aspecte privind securitatea naţională;

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

(2) 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.

(3) Prezentul Acord nu acoperă schimbul de informaţii în cadrul cooperării directe dintre serviciile de informaţii ale celor două Părţi, care va face obiectul unor acorduri separate.

ARTICOLUL 2
DEFINIŢII

În sensul prezentului Acord:

a) **Informaţie Clasificată** înseamnă:
orice informaţie, document sau material, indiferent de forma sa fizică şi căreia i s-a atribuit un nivel de clasificare de securitate în conformitate cu legile şi regulamentele naţionale şi care va fi protejată corespunzător;

b) **Document Clasificat** înseamnă:
orice tip de înregistrare ce conţine informaţii clasificate indiferent de formă sau caracteristică fizică, incluzând, dar fără a se limita la, materiale scrise sau tipărite, cartele şi benzi de procesare a datelor, hărţi, grafice, fotografii, picturi, desene, gravuri, schiţe, note şi documente de lucru,

copii la indigo şi riboane de printare sau reproduceri efectuate prin orice mijloace sau metode, înregistrări audio, vocale, magnetice sau electronice, optice sau video sub orice formă, cât şi echipamente portabile de procesare automată a datelor cu medii fixe de stocare şi detaşabile;

c) **Material Clasificat** înseamnă:
orice obiect sau parte a unui mecanism, prototip, echipament, armă, realizat mecanic sau manual, fabricat sau aflat în curs de fabricaţie, căruia i s-a atribuit un nivel de clasificare de securitate;

d) **Nivel de Clasificare de Securitate** înseamnă:
categorie care, în conformitate cu legile şi regulamentele naţionale, indică importanţa informaţiilor clasificate şi determină anumite restricţii privind accesul la aceste informaţii, măsurile de protecţie şi marcajul;

e) **Contract Clasificat** înseamnă:
un acord între doi sau mai mulţi contractori, prin care se stabilesc şi se definesc drepturile şi obligaţiile părţilor şi care conţine sau implică informaţii clasificate;

f) **Contractor** sau **Sub-Contractor** înseamnă:
orice persoană fizică sau persoană juridică de drept public sau privat, care are capacitatea legală de a încheia contracte clasificate;

g) **Incident de Securitate** înseamnă:
o acţiune sau omisiune contrară legilor şi regulamentelor naţionale, care are ca rezultat compromiterea efectivă sau o posibilă compromitere a informaţiilor clasificate;

h) **Compromiterea Informațiilor Clasificate** înseamnă:
o situație în care - datorită unui incident de securitate sau a unei activități ostile (precum spionaj, act de terorism sau furt) informațiile clasificate şi-au pierdut confidențialitatea. Aceasta include pierderea, dezvăluirea parțială sau totală, modificarea şi distrugerea neautorizate ale informațiilor clasificate;

i) **Certificat de Securitate a Personalului** înseamnă:
un document care atestă faptul că, în îndeplinirea sarcinilor de serviciu, deținătorul este autorizat să aibă acces la informații clasificate de un anumit nivel de clasificare de securitate, în conformitate cu principiul necesității de a cunoaşte;

j) **Certificat de Securitate Industrială** înseamnă:
un document care atestă faptul că o persoană juridică este autorizată să încheie şi să deruleze un contract clasificat;

k) **Necesitatea de a cunoaşte** înseamnă:
principiul conform căruia accesul la informații clasificate se acordă numai acelor persoane care, în îndeplinirea sarcinilor de serviciu, trebuie să lucreze cu astfel de informații sau să aibă acces la acestea;

l) **Autoritatea Națională de Securitate** înseamnă:
autoritatea care răspunde de implementarea şi controlul măsurilor prevăzute în prezentul Acord. Aceste autorități sunt menționate în art. 6;

m) **Autoritate Desemnată de Securitate** înseamnă:
instituția care, în conformitate cu legile şi regulamentele naționale ale Părților, este abilitată să stabilească, pentru domeniul său de activitate şi responsabilitate, structuri şi măsuri proprii privind coordonarea şi controlul activității referitoare la protecția informațiilor clasificate;

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

ARTICOLUL 3
PROTECȚIA INFORMAȚIILOR CLASIFICATE

(1) În conformitate cu legile şi regulamentele lor naționale, Părțile vor lua măsuri corespunzătoare pentru protecția informațiilor clasificate transmise, primite, produse sau elaborate, ca rezultat al oricărui acord sau relație între entitățile publice sau private din statele lor. Părțile vor asigura aceeaşi protecție pentru informațiile clasificate schimbate, primite, produse sau elaborate, ca şi pentru informațiile clasificate naționale, potrivit nivelului de clasificare de securitate.

(2) Fiecare Parte va lua măsuri ca informațiile clasificate primite de la cealaltă Parte să fie folosite în scopul pentru care acestea au fost transmise.

(3) Partea primitoare şi persoanele juridice de drept public sau privat din statul său nu vor atribui un nivel mai scăzut de clasificare de

securitate pentru informațiile clasificate primite şi nici nu vor declasifica aceste informații, fără acordul prealabil scris al Autorității Naționale de Securitate a Părții emitente. Autoritatea Națională de Securitate a Părții emitente va informa Autoritatea Națională de Securitate a Părții primitoare asupra oricăror modificări survenite în nivelul de clasificare de securitate a informațiilor transmise.

(4) Documentele clasificate primite, marcate cu nivelul de clasificare de securitate STRICT SECRET DE IMPORTANȚĂ DEOSEBITĂ / TÄIESTI SALAJANE sau STRICT SECRET / SALAJANE vor fi multiplicate sau traduse numai cu acordul scris al Părții emitente. Toate multiplicările documentelor clasificate vor fi marcate cu acelaşi nivel de clasificare de securitate ca şi exemplarul original şi vor fi protejate în acelaşi mod ca şi informațiile originale. Numărul copiilor se va limita la numărul necesar pentru scopurile oficiale.

(5) Informațiile clasificate marcate cu nivelul de clasificare de securitate STRICT SECRET / SALAJANE sau SECRET / KONFIDENTSIAALNE vor fi distruse cu consimțământul scris sau la cererea Părții emitente în conformitate cu legile şi regulamentele naționale ale Părții primitoare, astfel încât să nu fie posibilă reconstituirea totală sau parțială a acestora.

(6) Partea primitoare va informa Partea emitentă cu privire la distrugerea informațiilor clasificate. Informațiile STRICT SECRET DE IMPORTANȚĂ DEOSEBITĂ / TÄIESTI SALAJANE nu vor fi distruse, ci vor fi returnate Părții emitente.

(7) În cazul unui pericol iminent, informațiile clasificate vor fi distruse fără autorizare prealabilă. Autoritatea Națională de Securitate a Părții emitente va fi imediat informată asupra acestui fapt.

(8) Accesul la informații clasificate este permis, cu respectarea principiului necesității de a cunoaşte, numai persoanelor autorizate sau care posedă Certificat de Securitate a Personalului valabil pentru nivelul de clasificare de securitate a informațiilor pentru care se solicită accesul.

(9) Nici una dintre Părți nu va transmite unui terț informațiile clasificate primite, fără acordul prealabil scris al Autorității Naționale de Securitate a Părții emitente. Prezentul Acord nu va fi invocat de nici una dintre Părți în scopul obținerii informațiilor clasificate pe care cealaltă Parte le-a primit de la un terț.

(10) Fiecare Parte va urmări aplicarea legilor şi regulamentelor de securitate în cadrul entităților de drept public şi privat care dețin, elaborează, produc şi/sau utilizează informații clasificate provenite din statul celeilalte Părți, prin intermediul vizitelor de inspecție,

ARTICOLUL 4

ECHIVALENȚA NIVELURILOR DE CLASIFICARE DE SECURITATE

(1) Părțile au stabilit următoarea echivalență a nivelurilor naționale de clasificare de securitate:

România	Republica Estonia	Echivalentul în Engleză
STRICT SECRET DE IMPORTANȚĂ DEOSEBITĂ	TÄIESTI SALAJANE	TOP SECRET
STRICT SECRET	SALAJANE	SECRET
SECRET	KONFIDENTSIAALNE	CONFIDENTIAL
SECRET DE SERVICU	PIIRATUD	RESTRICTED

(2) Ambele Părți vor marca toate informațiile clasificate primite de la cealaltă Parte cu nivelul național de clasificare de securitate corespunzător, conform alin.(1).

ARTICOLUL 5
ACCESUL LA INFORMAȚII CLASIFICATE

(1) Înainte ca una dintre Părți să furnizeze informații clasificate unui reprezentant al celeilalte Părți, Autoritatea Națională de Securitate a Părții primitoare va informa în scris Autoritatea Națională de Securitate a Părții emitente că acesta este autorizat să aibă acces la informații clasificate, sau că deține Certificat de Securitate a Personalului corespunzător celui mai înalt nivel de clasificare de securitate a informațiilor la care urmează să aibă acces.

(2) Certificatul de Securitate a Personalului se va acorda după verificarea de securitate, în conformitate cu legile şi regulamentele naţionale ale fiecărei Părţi.

(3) La cerere, Autorităţile Naţionale de Securitate/Autorităţile Desemnate de Securitate ale Părţilor, respectând legile şi regulamentele naţionale, îşi vor acorda asistenţă reciprocă în cazul procedurilor de vetting legate de emiterea Certificatelor de Securitate a Personalului şi a Certificatelor de Securitate Industrială. În acest sens, se pot încheia aranjamente specifice între Autorităţile Naţionale de Securitate/Autorităţile Desemnate de Securitate ale Părţilor.

(4) Părţile îşi vor recunoaşte reciproc Certificatele de Securitate a Personalului şi Certificatele de Securitate Industrială emise conform legilor şi regulamentelor din statele lor.

(5) Autorităţile Naţionale de Securitate se vor informa reciproc asupra oricăror modificări ale Certificatelor de Securitate a Personalului şi Certificatelor de Securitate Industrială, în special asupra cazurilor de retragere a acestora.

ARTICOLUL 6
AUTORITĂŢILE NAŢIONALE DE SECURITATE

(1) Autorităţile Naţionale de Securitate ale Părţilor sunt:

În România	În Republica Estonia
Guvernul României Oficiul Registrului Național al Informațiilor Secrete de Stat Str. Mureş nr. 4, Sector 1 Bucureşti ROMÂNIA	Eesti riigi julgeoleku volitatud esindaja Julgeolekuosakond Kaitseministeerium Sakala 1 15094 Tallinn EESTI

(2) Autoritățile Naționale de Securitate își vor furniza reciproc, la cerere, informații referitoare la organizarea şi procedurile lor de securitate. În acest sens, Autoritățile Naționale de Securitate vor cădea de acord şi asupra vizitelor reciproce.

ARTICOLUL 7
VIZITELE

(1) Vizitele ce implică acces la informațiile clasificate privind activitățile descrise în art.1 vor fi aprobate de Autoritatea Națională de Securitate/Autoritatea Desemnată de Securitate a statului respectiv pentru vizitatorii din statul celeilalte Părți.

(2) Procedurile legate de vizite vor fi stabilite şi convenite între Autoritățile Naționale de Securitate/Autoritățile Desemnate de Securitate.

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

ARTICOLUL 8
CONTRACTELE CLASIFICATE

(1) În cazul în care una dintre Părți sau o entitate de drept public ori privat din statul său intenționează să încredințeze un contract clasificat ce urmează a se derula pe teritoriul statului celeilalte Părți, Partea din statul în care se derulează contractul îşi va asuma responsabilitatea de a proteja informațiile clasificate legate de contract, în conformitate cu legile şi regulamentele proprii.

(2) Înainte de diseminarea către contractori/sub-contractori sau potențiali contractori/sub-contractori a oricăror informații clasificate primite de la cealaltă Parte, Partea primitoare va trebui:

a) să acorde Certificate de Securitate Industrială de nivel corespunzător contractorilor/sub-contractorilor sau potențialilor contractori/sub-contractori, cu condiția ca aceştia să fi îndeplinit cerințele necesare eliberării certificatului;

b) să acorde Certificate de Securitate a Personalului de nivel corespunzător întregului personal ale cărui îndatoriri necesită acces la informații clasificate cu condiția ca aceste persoane să fi îndeplinit cerințele necesare eliberării certificatului.

(3) Părțile se vor asigura că fiecare contract clasificat conține şi o secțiune în care sunt definite cerințele de securitate sau acele elemente ale contractului ce necesită protecție de securitate precum şi o listă a informațiilor clasificate, materialelor şi activităților legate de contractul clasificat cu nivelurile de clasificare de securitate ale acestora.

(4) Procedurile referitoare la contractele clasificate vor fi elaborate şi convenite de către Autorităţile Naţionale de Securitate ale Părţilor.

(5) Părţile vor asigura protecţia drepturilor de autor, drepturilor de proprietate industrială – inclusiv a brevetelor de invenţii – şi a oricăror alte drepturi legate de informaţiile clasificate schimbate între statele lor, conform propriilor legi şi regulamente naţionale.

ARTICOLUL 9
TRANSMITEREA INFORMAŢIILOR CLASIFICATE

(1) Informaţiile Clasificate se vor transmite prin canale diplomatice sau curier militar ori prin alte mijloace acceptate de Autorităţile Naţionale de Securitate. Autoritatea Naţională de Securitate primitoare va confirma primirea informaţiilor clasificate.

(2) Dacă există un volum mare de informaţii clasificate ce trebuie transmis, Autorităţile Naţionale de Securitate vor conveni asupra mijloacelor de transport, traseului şi măsurilor de securitate pentru fiecare caz în parte.

(3) Se pot utiliza şi alte mijloace autorizate de transmitere sau schimb de informaţii clasificate, dacă sunt convenite de către Autorităţile Naţionale de Securitate.

(4) Transmiterea electromagnetică a informaţiilor clasificate se va efectua numai sub formă criptată cu echipamente criptografice aprobate de Autorităţile Naţionale de Securitate.

ARTICOLUL 10
INCIDENTE DE SECURITATE

(1) În cazul producerii unui incident de securitate care determină compromiterea sau posibila compromitere a informațiilor clasificate, Autoritatea Națională de Securitate din statul în care s-a produs incidentul de securitate va informa imediat Autoritatea Națională de Securitate a celeilalte Părți, va asigura investigația de securitate adecvată a acestui caz şi va lua măsurile necesare de limitare a consecințelor, în conformitate cu legile şi regulamentele naționale. La cerere, Autoritățile Naționale de Securitate vor coopera la investigație.

(2) În cazul în care compromiterea se produce într-un stat terț, Autoritatea Națională de Securitate din statul Părții emitente va acționa conform celor menționate în alin.(1).

(3) După încheierea investigațiilor, Autoritatea Națională de Securitate a Părții pe teritoriul căreia a avut loc compromiterea sau posibila compromitere a informațiilor clasificate va comunica imediat, în scris, prin intermediul Autorității Naționale de Securitate a celeilalte Părți rezultatele şi concluziile investigației.

ARTICOLUL 11
SOLUȚIONAREA DIFERENDELOR

Orice diferend privind interpretarea sau aplicarea prezentului Acord se va soluționa prin consultări între Autoritățile Naționale de Securitate sau, dacă nu se poate ajunge la o soluționare acceptabilă, între reprezentanții desemnați ai Părților.

ARTICOLUL 12
CHELTUIELI

Fiecare Parte va suporta eventualele cheltuieli legate de implementarea prezentului Acord în conformitate cu legile şi regulamentele naţionale.

ARTICOLUL 13
ASISTENŢĂ RECIPROCĂ

(1) Fiecare Parte va acorda asistenţă personalului din statul celeilalte Părţi pentru implementarea şi interpretarea prezentului Acord.

(2) Dacă este nevoie, Autorităţile Naţionale de Securitate se vor consulta reciproc asupra unor aspecte tehnice specifice privind implementarea prezentului Acord şi pot conveni de comun acord asupra încheierii unor protocoale de securitate suplimentare, speciale, la acest Acord, de la caz la caz.

ARTICOLUL 14
DISPOZIŢII FINALE

(1) Prezentul Acord este încheiat pe perioadă nedeterminată şi este supus aprobării în conformitate cu procedurile naţionale legale din statele Părţilor.

(2) Prezentul Acord va intra în vigoare în prima zi a celei de-a doua luni care urmează după primirea ultimei notificări între Părți prin care se menționează că au fost încheiate procedurile legale interne, necesare intrării în vigoare a acestui Acord.

(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 cealaltă Parte a primit notificarea de denunțare.

(4) Fără a ține cont de încetarea valabilității prezentului Acord, toate informațiile clasificate furnizate în baza prezentului Acord vor continua să fie protejate în conformitate cu prevederile acestuia.

(5) Prezentul Acord poate fi amendat pe baza consimțământului reciproc al Părților. Amendamentele vor intra în vigoare în conformitate cu prevederile alin.(2).

(6) Fiecare Parte va notifica prompt celeilalte Părți toate modificările intervenite în legislația şi regulamentele naționale care ar putea afecta protecția informațiilor clasificate la care se referă prezentul Acord. În acest caz, Părțile se vor consulta pentru a lua în considerare posibilele modificări ale prezentului Acord. În tot acest 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 30 august 2006, în două exemplare originale, fiecare în limbile română, estonă şi engleză, toate textele fiind egal autentice. În caz de diferenţe în interpretare, textul în limba engleză va prevala.

PENTRU	PENTRU
GUVERNUL ROMÂNIEI	**GUVERNUL REPUBLICII ESTONIA**
Prof. dr. MARIUS PETRESCU	**HERMAN SIMM**
Secretar de Stat	**Directorul**
Directorul General	**Departamentului de Securitate**
al Oficiului Registrului Naţional al Informaţiilor Secrete de Stat	**Ministerul Apărării**

Rumeenia valitsuse ja Eesti Vabariigi valitsuse salastatud teabe vastastikuse kaitse kokkulepe

Rumeenia valitsus ja Eesti Vabariigi valitsus, edaspidi "pooled",

soovides kaitsta salastatud teavet, mida vahetavad pooled omavahel või teised riigiasutused või avalik- või eraõiguslikud isikud, kes tegelevad teise poole salastatud teabega, mida vahetatakse poolte julgeoleku volitatud esindajate vastutusalas toimuva tegevuse raames,

on kokku leppinud järgmises.

ARTIKKEL 1

KOHALDATAVUS

1. Kokkulepe on järgmistes küsimustes aluseks igasugusele tegevusele, mis kooskõlas riigisiseste õigusaktidega on seotud salastatud teabe vahetamisega poolte või teiste riigiasutuste või avalik- või eraõiguslike isikute vahel:

a) poolte koostöö riigikaitse- ja muudes riigi julgeolekuga seotud küsimustes;

b) poolte riigiasutuste või avalik- või eraõiguslike isikute koostöö, ühisettevõtted, lepingud või muud suhted riigikaitsevaldkonnas ja muudes riigi julgeolekuga seotud küsimustes;

c) varustuse, toodete ja oskusteabe müük.

2. Kokkulepe ei mõjuta kummagi poole muudest rahvusvahelistest kokkulepetest tulenevaid kohustusi ning seda ei kasutata teiste riikide huvide, julgeoleku ega territoriaalse terviklikkuse vastu.

3. Kokkulepe ei käsitle poolte julgeolekuasutuste koostööga seotud teabevahetust, mida reguleeritakse eraldi kokkulepetega.

ARTIKKEL 2

MÕISTED

Kokkuleppes kasutatakse järgmisi mõisteid:

a) *Salastatud teave* – mis tahes vormis teave, dokument või materjal, millele on kooskõlas riigisiseste õigusaktidega määratud salastatuse tase ning mida kaitstakse vastavalt sellele.

b) *Salastatud dokument* – mis tahes vormis või füüsiliste omadustega salvestis, mis sisaldab salastatud teavet, sealhulgas käsikirjad ja trükised, automaatse andmetöötluse kaardid ja lindid, plaanid, graafikud, fotod, maalid, joonistused, graveeringud, visandid, märkmed ja mustandid, kopeerid ja tindilindid või mis tahes vahendite või meetodite abil valmistatud paljundused, mis tahes kujul heli-, hääl-, magnet- või elektron- või optilised või videosalvestised ja kaasaskantavad automaatsed andmetöötlusseadmed koos püsi- ning irdmäluga.

c) *Salastatud materjal* – esemed või masinate, prototüüpide, seadmete ja relvade käsitsi või tööstuslikult valmistatud või tootmisjärgus osised, millele on määratud salastatuse tase.

d) *Salastatuse tase* – kategooria, mis kooskõlas riigisiseste õigusaktidega iseloomustab salastatud teabe tähtsust ja kehtestab sellele juurdepääsu piirangud ning selle kaitsmiseks ja märgistamiseks võetavad meetmed.

e) *Salastatud leping* – kahe või enama lepinglase kokkulepe, millega nähakse ette nendevahelised õigused ja kohustused ning mis sisaldab salastatud teavet või on sellega seotud.

f) *Lepinglane või lepinglasest alltöövõtja* – füüsiline või avalik- või eraõiguslik juriidiline isik, kellel on õigus sõlmida salastatud lepinguid.

g) *Salastatud teabe kaitse nõuete rikkumine* – tegevus või tegevusetus, mis on vastuolus riigisiseste õigusaktidega ja mille tõttu salastatud teave satub või võib sattuda ohtu.

h) *Salastatud teabe ohtusattumine* – olukord, kus salastatud teave on selle kaitse nõuete rikkumise või kuritahtliku tegevuse (näiteks spionaaž, terroriakt või vargus) tõttu kaotanud salastatuse. Salastatud teave loetakse ohtu sattunuks, kui see on kadunud, osaliselt või täielikult avalikustatud, loata muudetud või loata hävitatud.

i) *Füüsilise isiku juurdepääsuluba* – dokument, mis tõendab, et selle valdajal on tööülesannete ja põhjendatud teadmisvajaduse tõttu juurdepääsuõigus teatud salastatuse tasemega salastatud teabele.

j) *Juriidilise isiku juurdepääsuluba* – dokument, mis tõendab, et juriidiline isik on volitatud sõlmima ja täitma salastatud lepinguid.

k) *Põhjendatud teadmisvajadus* – põhimõte, mille kohaselt juurdepääs salastatud teabele võimaldatakse üksnes isikutele, kellel on seda vaja seoses oma tööülesannete täitmisega.

l) *Riigi julgeoleku volitatud esindaja* – asutus, mis vastutab kokkuleppest tulenevate meetmete võtmise ja kontrollimise eest. Sellised asutused on loetletud artiklis 6.

m) *Määratud julgeolekuasutus* – asutus, mis kooskõlas poolte riigisiseste õigusaktidega on volitatud looma oma tegevusvaldkonnas ja pädevusalas salastatud teabe kaitse koordineerimise ja juhtimisega seotud struktuure ja võtma meetmeid.

n) *Kolmas isik* – üksikisik, asutus, riiklik või rahvusvaheline organisatsioon, avalik- või eraõiguslik isik, kes ei ole kokkuleppe pool.

ARTIKKEL 3

SALASTATUD TEABE KAITSMINE

1. Pooled võtavad kooskõlas riigisiseste õigusaktidega meetmeid, et kaitsta salastatud teavet, mida edastatakse, saadakse, koostatakse või töötatakse välja tulenevalt poolte füüsiliste või juriidiliste isikute vahelistest kokkulepetest või suhetest. Pooled tagavad vahetatud, saadud, koostatud või välja töötatud salastatud teabele samasuguse kaitse nagu oma samaväärsel tasemel salastatud teabele.

2. Pool tagab, et kasutab teiselt poolelt saadud salastatud teavet otstarbel, milleks see talle anti.

3. Vastuvõttev pool ning selle avalik- ja eraõiguslikud isikud ei vähenda saadud salastatud teabe salastatuse taset ega kustuta teabe salastatust ilma päritolupoole julgeoleku volitatud esindaja eelneva kirjaliku nõusolekuta. Päritolupoole julgeoleku

volitatud esindaja teatab vastuvõtva poole julgeoleku volitatud esindajale kõigist edastatud teabe salastatuse taseme muudatustest.

4. Vastuvõetud salastatud dokumente, mis on märgistatud salastatuse tasemega "STRICT SECRET DE IMPORTANȚĂ DEOSEBITĂ" / "TÄIESTI SALAJANE", paljundatakse ja tõlgitakse üksnes päritolupoole kirjalikul nõusolekul. Salastatud dokumentide kõigile koopiatele märgitakse sama salastatuse tase nagu originaaleksemplarile ning neid kaitstakse originaaliga võrdväärselt. Koopiaid tehakse üksnes ametlikuks otstarbeks vajalikul hulgal.

5. Salastatud teave, mis on märgistatud salastatuse tasemega "SECRET" / "KONFIDENTSIAALNE" või "STRICT SECRET" / "SALAJANE", hävitatakse päritolupoole kirjalikul nõusolekul või taotlusel kooskõlas vastuvõtva poole riigisiseste õigusaktidega nii, et seda ei ole võimalik ei osaliselt ega täielikult taastada.

6. Vastuvõttev pool teatab päritolupoolele salastatud teabe hävitamisest. Salastatud teavet, mis on märgistatud salastatuse tasemega "STRICT SECRET DE IMPORTANȚĂ DEOSEBITĂ" / "TÄIESTI SALAJANE", ei hävitata, vaid tagastatakse päritolupoolele.

7. Otsese ohu korral hävitatakse salastatud teave luba või nõusolekut taotlemata. Sellest teatatakse viivitamata päritolupoole julgeoleku volitatud esindajale.

8. Juurdepääs salastatud teabele võimaldatakse põhjendatud teadmisvajaduse korral üksnes isikutele, kellel on selleks õigus või kellel on taotletava teabe salastatuse tasemele vastav juurdepääsuluba.

9. Pool ei loovuta saadud salastatud teavet kolmandatele isikutele ilma päritolupoole julgeoleku volitatud esindaja eelneva kirjaliku nõusolekuta. Kumbki pool ei kasuta kokkulepet selleks, et saada salastatud teavet, mida teine pool on saanud kolmandatelt isikutelt.

10. Pooled kontrollivad kontrollivisiitide abil julgeolekunõuete täitmist avalik- ja eraõiguslike isikute poolt, kelle valduses on teise poole salastatud teavet või kes seda välja töötavad, koostavad ja/või kasutavad.

ARTIKKEL 4

SALASTATUSE TASEMETE VÕRDVÄÄRSUS

1. Pooled on kokku leppinud, et järgmised salastatuse tasemed on võrdväärsed:

Rumeenia	Eesti Vabariik	Ingliskeelne vaste
STRICT SECRET DE IMPORTANȚĂ DEOSEBITĂ	TÄIESTI SALAJANE	TOP SECRET
STRICT SECRET	SALAJANE	SECRET
SECRET	KONFIDENTSIAALNE	CONFIDENTIAL
SECRET DE SERVICIU	PIIRATUD	RESTRICTED

2. Pool märgistab teiselt poolelt saadud salastatud teabe kooskõlas lõikes 1 nimetatud vastava riigisisese salastatuse tasemega.

ARTIKKEL 5

JUURDEPÄÄS SALASTATUD TEABELE

1. Enne salastatud teabe üleandmist teise poole esindajale teatab vastuvõtva poole julgeoleku volitatud esindaja päritolupoole julgeoleku volitatud esindajale kirjalikult, et isikul, kes teabe vastu võtab, on salastatud teabele juurdepääsu õigus või asjakohase teabe kõrgeimat salastatuse taset hõlmav juurdepääsuluba.

2. Füüsilise isiku juurdepääsuluba antakse pärast julgeolekukontrolli, mis tehakse kooskõlas mõlema poole riigisiseste õigusaktidega.

3. Poolte julgeoleku volitatud esindajad või määratud julgeolekuasutused aitavad asjakohase taotluse korral ja riigisisestest õigusaktidest lähtudes teineteist füüsiliste ja juriidiliste isikute juurdepääsulubade väljastamisega seotud kontrollimisel. Poolte julgeoleku volitatud esindajad või määratud julgeolekuasutused võivad selleks sõlmida eraldi kokkuleppeid.

4. Pooled tunnustavad vastastikku kooskõlas riigisiseste õigusaktidega väljastatud füüsiliste ja juriidiliste isikute juurdepääsulube.

5. Poolte julgeoleku volitatud esindajad teatavad teineteisele kõigist muudatustest seoses füüsiliste ja juriidiliste isikute juurdepääsulubadega, eeskätt aga nende tühistamisest.

ARTIKKEL 6

RIIGI JULGEOLEKU VOLITATUD ESINDAJAD

1. Poolte julgeoleku volitatud esindajad on järgmised:

Rumeenias	Eesti Vabariigis
Rumeenia valitsus Salastatud Teabe Riiklik Registriamet 4 Mures Street, district 1 Bucharest ROMANIA	Eesti riigi julgeoleku volitatud esindaja Julgeolekuosakond Kaitseministeerium Sakala 1 15094 Tallinn EESTI

2. Poolte julgeoleku volitatud esindajad annavad teineteisele asjakohase taotluse korral teavet oma julgeolekukorralduse kohta. Selleks lepivad riikide julgeoleku volitatud esindajad kokku ka vastastikustes külastustes.

ARTIKKEL 7

KÜLASTUSED

1. Poolte kodanike vastastikused külastused, millega kaasneb juurdepääsuvajadus salastatud teabele seoses artiklis 1 nimetatud tegevusega, kiidab heaks vastuvõtva poole julgeoleku volitatud esindaja või määratud julgeolekuasutus.

2. Poolte julgeoleku volitatud esindajad või määratud julgeolekuasutused töötavad välja ja kooskõlastavad omavahel külastuskorra.

3. Pool tagab külastajate isikuandmete kaitsmise asjakohaste riigisiseste õigusaktide kohaselt.

ARTIKKEL 8

SALASTATUD LEPINGUD

1. Kui pool või selle avalik- või eraõiguslik isik kavatseb sõlmida salastatud lepingu, mida tuleb täita teise poole territooriumil, võtab vastutuse lepinguga seotud salastatud teabe kaitsmise eest kooskõlas oma riigisiseste õigusaktidega see pool, kelle territooriumil lepingut täitma hakatakse.

2. Enne teiselt poolelt saadud salastatud teabe edastamist kindlaksmääratud või võimalikele lepinglastele või lepinglastest alltöövõtjatele teeb vastuvõttev pool järgmist:

a) väljastab kindlaksmääratud või võimalikele lepinglastele või lepinglastest alltöövõtjatele asjakohase salastatuse tasemega juriidilise isiku juurdepääsuload, kui nende väljastamise tingimused on täidetud;

b) väljastab kõigile töötajatele, kes vajavad juurdepääsu salastatud teabele seoses oma tööülesannetega, füüsilise isiku juurdepääsuloa, kui selle väljastamise tingimused on täidetud.

3. Pooled tagavad, et igas salastatud lepingus on kindlaks määratud julgeolekunõuded või lepingu need osad, mida tuleb kaitsta, ning esitatud lepinguga seotud salastatud teabe, materjali ja tegevuse loend koos asjakohaste salastatuse tasemetega.

4. Poolte julgeoleku volitatud esindajad töötavad välja ja kooskõlastavad omavahel salastatud lepingutega seotud korra.

5. Pooled tagavad autoriõiguste, tööstusomandiõiguste (sealhulgas patendid) ja omavahel vahetatava salastatud teabega seotud muude õiguste kaitsmise oma riigisiseste õigusaktide kohaselt.

ARTIKKEL 9

SALASTATUD TEABE EDASTAMINE

1. Salastatud teavet edastatakse diplomaatiliste kanalite kaudu, sõjaväekullerite abil või muul, riikide julgeoleku volitatud esindajate kokku lepitud viisil. Vastuvõtva poole julgeoleku volitatud esindaja kinnitab salastatud teabe kättesaamist.

2. Suure koguse salastatud teabe edastamisel lepivad poolte julgeoleku volitatud esindajad iga kord eraldi kokku transpordivahendites, marsruudis ning julgeolekumeetmetes.

3. Poolte julgeoleku volitatud esindajate vastastikusel kokkuleppel võib salastatud teabe edastamiseks ja vahetamiseks kasutada ka muid lubatud vahendeid.

4. Salastatud teavet edastatakse elektrooniliselt üksnes krüpteeritud kujul, mille krüpteerimiseks kasutatud krüptoseadmed on heaks kiitnud poolte julgeoleku volitatud esindajad.

ARTIKKEL 10

SALASTATUD TEABE KAITSE NÕUETE RIKKUMINE

1. Salastatud teabe kaitse nõuete rikkumise korral, mille tulemusel salastatud teave satub või võib sattuda ohtu, teatab selle poole julgeoleku volitatud esindaja, kelle territooriumil rikkumine toimus, juhtunust viivitamata teise poole julgeoleku volitatud esindajale, tagab juhtunu nõuetekohase uurimise ning võtab kooskõlas oma riigisiseste õigusaktidega rikkumise tagajärgede piiramiseks vajalikke meetmeid. Vajaduse korral teevad poolte julgeoleku volitatud esindajad uurimisel koostööd.

2. Kui salastatud teave satub ohtu kolmandas riigis, võtab lõikes 1 nimetatud meetmeid päritolupoole julgeoleku volitatud esindaja.

3. Pärast uurimise lõpetamist teatab selle poole julgeoleku volitatud esindaja, kelle territooriumil salastatud teave sattus või võis sattuda ohtu, teise poole julgeoleku volitatud esindajale kirjalikult uurimise tulemustest ja järeldustest.

ARTIKKEL 11

VAIDLUSTE LAHENDAMINE

Vaidlused kokkuleppe tõlgendamise või täitmise üle lahendavad nõupidamise teel poolte julgeoleku volitatud esindajad või, kui sel viisil vastuvõetavat lahendust ei saavutata, poolte määratud esindajad.

ARTIKKEL 12

KULUD

Kumbki pool kannab enda kokkuleppe täitmisega seotud kulud kooskõlas oma riigisiseste õigusaktidega.

ARTIKKEL 13

VASTASTIKUNE ABISTAMINE

1. Pool abistab teise poole töötajaid kokkuleppe tõlgendamisel ja täitmisel.

2. Vajaduse korral peavad poolte julgeoleku volitatud esindajad teineteisega kokkuleppe täitmisega seotud konkreetsetes tehnilistes küsimustes nõu ning võivad vastastikusel kokkuleppel sõlmida konkreetseid julgeolekuaspekte reguleerivaid lisaprotokolle.

ARTIKKEL 14

LÕPPSÄTTED

1. Kokkulepe sõlmitakse määramata ajaks ning tuleb heaks kiita poolte riigisisese menetluskorra kohaselt.

2. Kokkulepe jõustub teise kuu esimesel päeval pärast seda, kui saabub viimane teise poole teade selle kohta, et kokkuleppe jõustumiseks vajalik riigisisene menetlus on lõppenud.

3. Poolel on õigus kokkulepe igal ajal lõpetada. Sellisel juhul kaotab kokkulepe kehtivuse kuus kuud pärast seda, kui üks pool teatas teisele poolele kokkuleppe lõpetamisest.

4. Kokkuleppe lõpetamisest olenemata kaitstakse kokkuleppe alusel saadud salastatud teavet ka edaspidi kokkuleppe kohaselt.

5. Poolte vastastikusel nõusolekul võib kokkulepet muuta. Muudatused jõustuvad lõike 2 kohaselt.

6. Pool teatab teisele poolele viivitamata oma riigisiseste õigusaktide muudatustest, mis võivad mõjutada kokkuleppe alusel vahetatava salastatud teabe kaitsmist. Sellisel juhul peavad pooled teineteisega nõu, et arutada kokkuleppe võimalikku muutmist. Seni kaitstakse salastatud teavet kokkuleppe kohaselt, välja arvatud juhul, kui päritolupool esitab kirjaliku taotluse toimida teisiti.

Koostatud Bukarestis 30. augustil 2006. aastal kahes võrdselt autentses eksemplaris rumeenia, eesti ja inglise keeles. Tõlgendamisest tulenevate erimeelsuste korral lähtutakse ingliskeelsest tekstist.

RUMEENIA VALITSUSE NIMEL

Prof.dr. MARIUS PETRESCU
Riigisekretär
Peadirektor
Salastatud Teabe Riiklik Registriamet

EESTI VABARIIGI VALITSUSE NIMEL

HERMAN SIMM
Osakonnajuhataja
Julgeolekuosakond
Kaitseministeerium

AGREEMENT

BETWEEN

THE GOVERNMENT OF ROMANIA

AND

THE GOVERNMENT OF THE REPUBLIC OF ESTONIA

ON MUTUAL PROTECTION OF CLASSIFIED INFORMATION

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

In order to safeguard the Classified Information exchanged directly between the Parties or other state bodies, public and private entities which deal with Classified Information of the state of the other Party and within the framework of activities which fall under the responsibility of the National Security Authorities of the Parties,

Have agreed as follows:

ARTICLE 1
APPLICABILITY

1. This Agreement shall form the basis of any activity, involving, in compliance with national laws and regulations, the exchange of Classified Information between the Parties or other state bodies or public and private entities, concerning the following:

a. co-operation between the Parties concerning the national defence 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 states of the Parties in the field of national defence and any other issue related to national security;

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

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

3. This agreement does not cover the exchange of information related to direct cooperation between intelligence services of both Parties which shall be subject to separate agreements.

ARTICLE 2
DEFINITIONS

For the purpose of this Agreement:

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

b. **Classified Document** means:
any sort of record containing Classified Information regardless of its form or physical characteristic, including, without limitation, written or printed

matters, data processing cards and tapes, maps, charts, photographs, paintings, drawings, engravings, sketches, working notes and papers, carbon copies and ink ribbons, or reproductions produced by any means or processes, and sound, voice, magnetic 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, mechanically or hand made manufactured or in process of manufacture, to which a Security Classification Level has been assigned;

d. **Security Classification Level** means:
category which, according to the national laws and regulations, characterises the importance of Classified Information and which determines certain restrictions of access to it, measures of protection and marking;

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 a legal public or private entity possessing the legal capability to conclude Classified Contracts;

g. **Breach of Security** means:
an act or omission contrary to national laws and regulations, 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. This includes loss, partial or total disclosure, unauthorized modification and unauthorised destruction of Classified Information;

i. **Personnel Security Clearance Certificate** means:
a document certifying that, in performing his/her duties, the holder is authorised to have access to Classified Information of a certain Security Classification Level, in compliance with the Need-to-know principle;

j. **Facility Security Clearance Certificate** means:
a document certifying that a legal entity is authorized to conclude and perform a Classified Contract;

k. **Need to know** means:
a principle by which access to Classified Information may be granted only to those persons who, in performing their duties, need to work with or have access to such information;

l. **National Security Authority** means:
the authority responsible for the implementation and the control of the measures undertaken under the provisions of this Agreement. Such authorities are listed in Article 6;

m. **Designated Security Authority** means:
the institution which, in compliance with the national laws and regulations 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;

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

ARTICLE 3
PROTECTION OF CLASSIFIED INFORMATION

1. In accordance with their national laws and regulations, 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 public or private entities of their respective states. The Parties shall ensure to all the exchanged, received, produced or developed Classified Information the same protection, as it is provided for the national Classified Information, with the corresponding Security Classification Level.

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.

3. The receiving Party and the public or private entities of its state shall neither assign a lower Security Classification Level for the received Classified Information nor declassify this information without the prior written consent of the National Security Authority of the originating Party. The National Security Authority of the originating Party shall inform the National Security Authority of the receiving Party of any changes in Security Classification Level of the transmitted information.

4. The received Classified Documents marked with a Security Classification Level STRICT SECRET DE IMPORTANȚĂ DEOSEBITĂ / TÄIESTI SALAJANE shall be reproduced or translated only with the written consent of the originating Party. All reproductions of Classified Documents shall be marked with the same Security Classification Level as the original copy and shall be protected in the same way as the original information. The number of copies shall limit to that number necessary for official purposes.

5. Classified Information marked with the Security Classification Level SECRET/ KONFIDENTSIAALNE or STRICT SECRET/SALAJANE shall be destroyed with the written consent of or at the request of the originating Party in accordance with the national laws and regulations of the receiving Party, in such a manner that any reconstruction in whole or in part be impossible.

6. The receiving Party shall inform the originating Party of the destruction of Classified Information. The STRICT SECRET DE IMPORTANȚĂ DEOSEBITĂ/ TĂIESTI SALAJANE information shall not be destroyed but returned to the originating Party.

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

8. Access to Classified Information is allowed, with the observance of the Need-to-know principle, only to those individuals authorised or having a Personnel Security Clearance Certificate valid for the Security Classification Level of the information for which the access is required.

9. None of the Parties shall release received Classified Information to a Third Party without prior written consent of the National Security Authority of the originating Party.
This Agreement shall not be invoked by either Party to obtain Classified Information that the other Party has received from a Third Party.

10. Each Party shall supervise the implementation of security laws and regulations at the public and private entities that hold, develop, produce and/or use Classified Information of the state of the other Party, by means of inspection visits.

ARTICLE 4
EQUIVALENCE OF SECURITY CLASSIFICATION LEVELS

1. The Parties have determined that the equivalence of the national Security Classification Levels is as follows:

Romania	Republic of Estonia	English Equivalent
STRICT SECRET DE IMPORTANȚĂ DEOSEBITĂ	TÄIESTI SALAJANE	TOP SECRET
STRICT SECRET	SALAJANE	SECRET
SECRET	KONFIDENTSIAALNE	CONFIDENTIAL
SECRET DE SERVICIU	PIIRATUD	RESTRICTED

2. Both Parties shall mark all the Classified Information received from the other Party with a corresponding national Security Classification Level according to paragraph (1).

ARTICLE 5
ACCESS TO CLASSIFIED INFORMATION

1. Before a Party provides Classified Information to a representative of the other Party, the National Security Authority of the receiving Party shall notify in writing the National Security Authority of the originating Party that he/she is authorised to have access to Classified Information or holds a

Personnel Security Clearance Certificate of the highest Security Classification Level for the information to which he/she is to have access.

2. The Personnel Security Clearance Certificate shall be granted following the security vetting conducted in accordance with the national laws and regulations of each Party.

3. On request, the National Security Authorities / Designated Security Authorities of the Parties, taking into account the respective national laws and regulations, shall assist each other in the vetting procedures related to the issue of the Personnel Security Clearance Certificates and of the Facility Security Clearance Certificates. To this end specific arrangements may be agreed upon between the National Security Authorities / Designated Security Authorities of the Parties.

4. The Parties shall mutually recognize the Personnel Security Clearance Certificates and Facility Security Clearance Certificates issued in accordance with the laws and regulations of their respective states.

5. The National Security Authorities shall inform each other of any changes to the Personnel Security Clearance Certificates and Facility Security Clearance Certificates, in particular of their revoke.

ARTICLE 6
NATIONAL SECURITY AUTHORITIES

1. The National Security Authorities of the Parties are:

In Romania	In the Republic of Estonia
Government of Romania National Registry Office for Classified Information 4 Mures Street, district 1 Bucharest ROMANIA	Estonian National Security Authority Security Department Ministry of Defence Sakala 1 15094 Tallinn ESTONIA

2. The National Security Authorities shall provide each other, upon request, with information about its security organization and procedures. To this end, the National Security Authorities shall also agree on mutual visits.

ARTICLE 7
VISITS

1. Visits involving access to Classified Information concerning the activities described in Article 1 shall be approved by the National Security Authority/Designated Security Authority of the respective state to visitors from the state of the other Party.

2. The procedures related to visits shall be developed and agreed upon between the National Security Authorities/Designated Security Authorities.

3. Each Party shall guarantee the protection of personal data of the visitors according to the national legislation in the field.

ARTICLE 8
CLASSIFIED CONTRACTS

1. In the event that any of the Party or public or private entities of its state intend to award a Classified Contract to be performed within the territory of the state of the other Party, 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 laws and regulations.

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 shall:

a. grant a Facility Security Clearance Certificate of an appropriate level to the Contractors/Sub-Contractors or to prospective Contractors/Sub-Contractors, on condition they have met the requirements for its issue;

b. grant Personnel Security Clearance Certificates of an appropriate level to all personnel whose duties require access to Classified Information on condition they have met the requirements for its issue.

3. The Parties shall ensure that every Classified Contract includes an appropriate part identifying the security requirements or those elements of the contract requiring security protection and a listing of Classified Information, materials and activities related to a Classified Contract and their Security Classification Levels.

4. The procedures related to Classified Contracts shall be developed and agreed upon between the National Security Authorities of the Parties.

5. The Parties shall ensure 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 laws and regulations.

ARTICLE 9
TRANSMISSION OF CLASSIFIED INFORMATION

1. Classified Information shall be transmitted through diplomatic channels or military courier or other means accepted by the National Security Authorities. The receiving National Security Authority shall confirm the receipt of Classified Information.

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

3. Other authorized means of transmission or exchange of Classified Information may be used, if agreed upon, by the National Security Authorities.

4. The electromagnetic transmission of Classified Information shall be carried out only in encrypted form by cryptographic equipment approved by the National Security Authorities.

ARTICLE 10
BREACH OF SECURITY

1. In case of a Breach of Security that results in a Compromise or possible Compromise of Classified Information, the National Security Authority of the state where the Breach of Security occurred shall promptly inform the National Security Authority of the other Party, ensure proper security investigation of such event and take the necessary measures to limit the consequences, in accordance with national laws and regulations. If required, the National Security Authorities shall cooperate in the investigation.

2. In case the Compromise occurs in a third country, the National Security Authority of the state of the originating Party shall take action as of paragraph 1.

3. After completion of investigation, the National Security Authority of the Party on the territory of which the Compromise or possible Compromise of Classified Information occurred shall immediately inform in writing, through

the National Security Authority of the other Party on the findings and conclusions of the investigation.

ARTICLE 11
SETTLEMENT OF DISPUTES

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

ARTICLE 12
COSTS

Each Party shall bear the eventual costs related to the implementation of this Agreement in accordance with national laws and regulations.

ARTICLE 13
MUTUAL ASSISTANCE

1. Each Party shall assist personnel from the state of the other Party in the implementation and interpretation of this Agreement.

2. Should the need arise the National Security Authorities 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 14
FINAL PROVISIONS

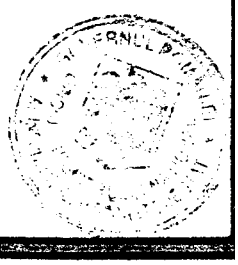
1. This Agreement is concluded for an indefinite period of time and is subject to approval in accordance with national legal procedures of the states of the Parties.

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 internal legal procedures necessary for this Agreement to enter into force have been completed.

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 termination was served to the other Party.

4. 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.

5. 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 2.



6. Each Party shall promptly notify the other Party of any changes to its national laws and regulations that would affect the protection of Classified Information under this Agreement. In such case, the Parties shall consult each other 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 30th of August 2006 in two original copies each in the Romanian, Estonian and English languages, all texts being equally authentic. In case of differences in the interpretation, the English text shall prevail.

FOR THE GOVERNMENT OF ROMANIA

Prof. dr. MARIUS PETRESCU

Secretary of State

Director General

of the National Registry Office for Classified Information

FOR THE GOVERNMENT OF THE REPUBLIC OF ESTONIA

HERMAN SIMM

Director

Security Department
Ministry of Defence