

Väljaandja: Vabariigi Valitsus
Akti liik: välisleping
Teksti liik: algtekst
Jõustumise kp: 01.09.2007
Avaldamismärge: RT II 2007, 15, 45

Eesti Vabariigi valitsuse ja Rumeenia valitsuse salastatud teabe vastastikuse kaitse kakkulepe

"Eesti Vabariigi valitsuse ja Rumeenia valitsuse salastatud teabe vastastikuse kaitse kakkuleppe" eelnõu heakskiitmine ja volituse andmine

Teadanne välislepingu jõustumise kohta

Koostatud Bukarestis 30. augustil 2006, jõustunud 1. septembril 2007

Eesti Vabariigi valitsus ja Rumeenia 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.

Artikel 1. Kohaldatavus

1. Kakkulepe on järgmistest 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. Kakkulepe ei mõjuta kummagi poole muudest rahvusvahelistest kakkulepetest tulenevaid kohustusi ning seda ei kasutata teiste riikide huvide, julgeoleku ega territoriaalse terviklikkuse vastu.
3. Kakkulepe ei käsitele poolte julgeolekuasutuste koostööga seotud teabevahetust, mida reguleeritakse eraldi kakkulepetega.

Artikel 2. Mõisted

Kakkuleppes 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 füüsiline omadustega salvestis, mis sisaldab salastatud teavet, sealhulgas käsikirjad ja trükised, automaatse andmetöötluuse 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 kakkulepe, millega nähakse ette nendevahelised õigused ja kohustused ning mis sisaldab salastatud teavet või on sellega seotud.
- f) Lepinglane või lepingglasest 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 juridiliseks salastatuseks – dokument, mis tõendab, et selle valdajal on tööülesannete ja põhjendatud teadmisvajaduse tõttu juridiliseks salastatuse tasemeega salastatud teabele.
- j) Juriidilise isiku juridiliseks salastatuseks – dokument, mis tõendab, et juriidiline isik on volitatud sõlmima ja täitma salastatud lepinguid.
- k) Põhjendatud teadmisvajadus – põhimõte, mille kohaselt juridilise 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.

Artikel 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. Vastuvõttes 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. Vastuvõtetud salastatud dokumente, mis on märgistatud salastatuse tasemeega «**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 võrdväärset. Koopiaid tehakse üksnes ametlikus otstarbeks vajalikul hulgjal.
5. Salastatud teave, mis on märgistatud salastatuse tasemeaga «**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. Vastuvõttes pool teatab päritolupoolele salastatud teabe hävitamisest. Salastatud teavet, mis on märgistatud salastatuse tasemeaga «**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 juridiliseks salastatuseks.
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.

Artikel 4. Salastatuse tasemete võrdväärus

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

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

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

Artikel 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 teatabud teineteisele kõigist muudatustest seoses füüsiliste ja juriidiliste isikute juurdepääsulubadega, eeskätt aga nende tühistamisest.

Artikel 6. Riigi julgeoleku volitatud esindajad

1. Poolte julgeoleku volitatud esindajad on järgmised:

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

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

Artikel 7. Külastused

1. Poolte kodanike vastastikused külastused, millega kaasneb juurdepääsuvajadus salastatud teabele seoses artiklis 1 nimetatud teevusega, 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.

Artikel 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 vastuvõtve 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 autorioiguste, tööstusomandiõiguste (sealhulgas patentid) ja omavahel vahetatava salastatud teabega seotud muude õiguste kaitsmise oma riigisisestesse õigusaktide kohaselt.

Artikel 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. Elektrooniliselt edastatakse salastatud teavet üksnes poolte julgeoleku volitatud esindajate heaks kiidetud krüpteeritud kujul.

Artikel 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, juhunust viivitamata teise poole julgeoleku volitatud esindajale, tagab juhtunu nõuetekohase uurimise ning võtab kooskõlas oma riigisisestesse 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.

Artikel 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.

Artikel 12. Kulud

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

Artikel 13. Vastastikune abistamine

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

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

Artikel 14. Lõppsätted

1. Kokkulepe sõlmítakse 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 kokkulepe 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 1 kohaselt.

6. Pool teatab teisele poolele viivitamata oma riigisisest 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 30. augustil 2006. a Bukarestis kahes võrdsest autentses eksemplaris eesti, rumeenia ja inglise keeles. Tõlgendamisest tulenevate erimeelsuste korral lähtutatakse ingliskeelsest tekstist.

Eesti Vabariigi valitsuse nimel
HERMANN SIMM
Osakonnajuhataja
Julgeolekuosakond
Kaitseministeerium

Rumeenia Valitsuse nimel
Prof.dr. MARIUS PETRESCU
Riigisekretär
Peadirektor
Salastatud Teabe Riiklik Registriamet

AGREEMENT BETWEEN THE GOVERNMENT OF THE REPUBLIC OF ESTONIA AND THE GOVERNMENT OF ROMANIA ON MUTUAL PROTECTION OF CLASSIFIED INFORMATION

The Government of the Republic of Estonia and the Government of Romania, 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 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/ TÄIESTI 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
TÄIESTI SALAJANE	STRICT SECRET DE IMPORTANȚĂ DEOSEBITĂ	TOP SECRET
SALAJANE	STRICT SECRET	SECRET
KONFIDENTSIAALNE	SECRET	CONFIDENTIAL
PIRATUD	SECRET DE SERVICIU	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 the Republic of Estonia
Estonian National Security Authority
Security Department
Ministry of Defence
Sakala 1

In Romania
Government of Romania
National Registry Office for Classified Information
4 Mures Street, district 1
Bucharest

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 1.
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 2007 in two original copies each in the Estonian, Romanian and English languages, all texts being equally authentic. In case of differences in the interpretation, the English text shall prevail.

For the Government of the Republic of Estonia
HERMANN SIMM
Director
Security Department
Ministry of Defence

For the Government of Romania
Prof Dr MARIUS PETRESCU
State Secretary
Director General
National Registry Office for Classified Information