Väljaandja:	Vabariigi Valitsus
Akti liik:	välisleping
Teksti liik:	algtekst
Jõustumise kp:	16.11.2008
Avaldamismärge:	RT II 2008, 30, 85

Eesti Vabariigi ja Portugali Vabariigi salastatud teabe kaitse kokkulepe

Alla kirjutatud 29. novembril 2005. a Lissabonis, jõustus 16. novembril 2008. a

Eesti Vabariik ja Portugali Vabariik,
edaspidi «pooled»,

tunnistades, et nad peavad tagama poolte ja nende füüsiliste või juriidiliste isikute vahel sõlmitud või sõlmitavate koostöökokkulepete või lepingute alusel vahetatava salastatud teabe kaitse;

soovides sätestada poolte vahetatava salastatud teabe vastastikuse kaitsmise korra,

on kokku leppinud järgmises.

Artikkel 1. Eesmärk

Kokkuleppega kehtestatakse salastatud teabe kaitse kord, mida kohaldatakse poolte pädevate asutuste või füüsiliste või juriidiliste isikute vahel sõlmitud või sõlmitavate koostöökokkulepete või lepingute suhtes, millega nähakse ette salastatud teabe vahetamine.

Artikkel 2. Kohaldamisala

1. Kokkuleppega sätestatakse poolte vahetatava salastatud teabe kaitse kord.

2. Kokkulepet ei kohaldata poolte julgeolekuasutuste otsekoostöö suhtes.

Artikkel 3. Mõisted

Kokkuleppes kasutatakse järgmisi mõisteid:
a) *salastatud teave*– teave, dokument või materjal, mida selle vormist, laadist ja edastamisviisist olenemata on vaja kaitsta loata avalikustamise eest ja millele on määratud salastatuse tase;
b) *riigi julgeoleku volitatud esindaja*– asutus, mille kumbki pool on määranud vastutavaks käesoleva kokkuleppe täitmise ja selle järelevalve eest;
c) *päritolupool*– pool, kes annab või edastab salastatud teavet teisele poolele;
d) *vastuvõttev pool*– pool, kellele päritolupool annab või edastab salastatud teavet;
e) *kolmas isik*– rahvusvaheline organisatsioon või riik, sealhulgas selle kodanikud ja juriidilised isikud, kes ei ole käesoleva kokkuleppe pool;
f) *lepinglane*– füüsiline või juriidiline isik, kellel on õigus sõlmida lepinguid;
g) *salastatud leping*– kahe või enama lepinglase kokkulepe, millega nähakse ette nende õigused ja kohustused ning mis sisaldab salastatud teavet või on sellega seotud;
h) *füüsilise isiku juurdepääsuluba*– riigi julgeoleku volitatud esindaja või muu pädeva asutuse poolt tehtud otsus, et füüsilisel isikul on salastatud teabele juurdepääsu õigus kooskõlas riigisiseste õigusaktidega;
i) *juriidilise isiku juurdepääsuluba*– riigi julgeoleku volitatud esindaja või muu pädeva asutuse otsus, et juriidiline isik on julgeolekust lähtudes reaalselt ja organisatsiooniliselt võimeline kasutama ja hoidma salastatud teavet kooskõlas riigisiseste õigusaktidega;
j) *põhjendatud teadmisvajadus* –salastatud teabele juurdepääsu võimaldamine üksnes isikule, kellel on tõestatud vajadus saada sellist teavet oma teenistus- ja ametikohustuste täitmiseks, milleks teave vastuvõtvale poolele anti või edastati;
k) *projekti julgeolekueeskiri*– julgeolekunõuded, mida kohaldatakse konkreetse projekti suhtes julgeolekukorra standardimiseks;

l) *projekti salastamisjuhend*– projekti julgeolekueeskirja see osa, milles määratakse projekti salastatud osad ja nende salastatuse tasemed.

Artikkel 4. Riigi julgeoleku volitatud esindaja

1. Riikide julgeoleku volitatud esindajad on järgmised:

Eesti Vabariigis:
Julgeolekuosakond, Kaitseministeerium, Sakala 1, 15094 Tallinn, EESTI;

Portugali Vabariigis:
Riigi julgeoleku volitatud esindaja, Ministrite nõukogu eesistuja, Av. Ilha da Madeira, 1; 1400-204 Lisbon, Portugal.

2. Pooled teatavad teineteisele diplomaatiliste kanalite kaudu oma julgeoleku volitatud esindajaid puudutavatest muudatustest.

Artikkel 5. Julgeolekupõhimõtted

1. Poolte vahetatava salastatud teabe kaitsmisel ja kasutamisel kehtivad järgmised põhimõtted:
a) pooled tagavad kogu edastatud, koostatud või väljatöötatud salastatud teabele samasuguse kaitse nagu oma samaväärsel tasemel salastatud teabele;
b) juurdepääs salastatud teabele võimaldatakse üksnes isikutele, kellel on põhjendatud teadmisvajadus; teabe puhul, mille salastatuse tase on KONFIDENTSIAALNE/CONFIDENCIAL või kõrgem, isikutele, kellel on pädevate asutuste väljastatud kehtiv juurdepääsuluba.

2. Võrreldaval tasemel kaitstuse saavutamiseks ja säilitamiseks annavad riikide julgeoleku volitatud esindajad asjakohase taotluse korral teineteisele teavet oma salastatud teabe kaitsmise õigusaktide, menetluskorra ja tavade kohta.

Artikkel 6. Salastatuse tasemed

1. Poolte kokkuleppel on järgmised salastatuse tasemed võrdväärsed ning vastavad nende riigisiseste õigusaktidega määratud salastatuse tasemetele:

Eesti Vabariik	Portugali Vabariik	Ingliskeelne vaste
TÄIESTI SALAJANE	MUITO SECRETO	TOP SECRET
SALAJANE	SECRETO	SECRET
KONFIDENTSIAALNE	CONFIDENCIAL	CONFIDENTIAL
PIIRATUD	RESERVADO	RESTRICTED

2. Vastuvõttev pool märgistab saadud salastatud teabe lõike 1 kohaselt salastatuse taseme omakeelse vastega.

3. Pooled teatavad teineteisele kõigist edastatud teabe salastatuse taseme muudatustest.

4. Vastuvõttev pool ei alanda saadud teabe salastatuse taset ega kustuta teabe salastatust ilma päritolupoole eelneva kirjaliku nõusolekuta.

Artikkel 7. Juurdepääsuload

1. Pooled aitavad oma julgeoleku volitatud esindajate kaudu asjakohase taotluse korral ja oma õigusaktidest lähtudes enne füüsiliste ja juriidiliste isikute juurdepääsulubade väljastamist teineteisel kontrollida oma riigi füüsilisi ja juriidilisi isikuid, kes elavad või asuvad teise poole territooriumil.

2. Pooled tunnustavad teise poole õigusaktide kohaselt väljastatud füüsiliste ja juriidiliste isikute juurdepääsulube. Juurdepääsulubade tasemed peavad olema kooskõlas artikliga 6.

3. Riikide julgeoleku volitatud esindajad teatavad teineteisele kõigist muudatustest seoses asjaomaste füüsiliste ja juriidiliste isikute juurdepääsulubadega, eeskätt nende tühistamisest või nende taseme alandamisest.

Artikkel 8. Tõlkimine, paljundamine ja hävitamine

1. Teavet, mille salastatuse tase on SALAJANE/SECRETO või kõrgem, paljundatakse ja tõlgitakse ainult päritolupoole julgeoleku volitatud esindaja kirjalikul loal.

2. Salastatud teavet tõlgitakse ja paljundatakse järgmise korra kohaselt:
a) asjaomastel isikutel peab olema artikli 5 nõuete kohane füüsilise isiku juurdepääsuluba;
b) tõlked ja paljundused märgistatakse ja kaitstakse võrdselt originaaliga;
c) tõlkeid ja paljundusi tehakse üksnes ametlike ülesannete täitmiseks vajalikus mahus;
d) tõlgetele lisatakse märge selles keeles, millesse ta on tõlgitud, selle kohta, et tõlge sisaldab päritolupoolelt saadud salastatud teavet.

3. Tasemel TÄIESTI SALAJANE / MUITO SECRETO salastatud teavet ei hävitata, vaid tagastatakse päritolupoole julgeoleku volitatud esindajale.

4. Tasemel SALAJANE/SECRETO salastatud teabe hävitamisest teatatakse päritolupoole julgeoleku volitatud esindajale.

5. Tasemel kuni KONFIDENTSIAALNE/CONFIDENCIAL (k.a) salastatud teave hävitatakse kooskõlas riigisiseste õigusaktidega.

6. Kriisiolukorras, kui käesoleva kokkuleppe alusel koostatud või edastatud salastatud teavet ei ole võimalik kaitsta ega tagastada, hävitatakse see kohe. Vastuvõttev pool teatab salastatud teabe hävitamisest päritolupoole julgeoleku volitatud esindajale võimalikult kiiresti.

Artikkel 9. Salastatud teabe edastamine

1. Pooled kasutavad salastatud teabe edastamiseks teineteisele oma julgeoleku volitatud esindajate poolt vastastikku heaks kiidetud kanaleid.

2. Pooled võivad salastatud teavet edastada elektrooniliselt, pidades kinni oma julgeoleku volitatud esindajate vahel kokkulepitud julgeolekunõuetest.

3. Suurte esemete ja mahuka salastatud teabe vahetamiseks annavad mõlema poole julgeoleku volitatud esindajad iga kord eraldi loa.

4. Vastuvõttev pool kinnitab salastatud teabe kättesaamist kirjalikult ning edastab selle kasutajatele.

Artikkel 10. Salastatud teabe kasutamine ja sellekohaste nõuete täitmine

1. Saadud salastatud teavet kasutatakse üksnes otstarbel, milleks see edastati.

2. Kumbki pool teatab salastatud teabega seotud olukordades oma füüsilistele ja juriidilistele isikutele käesoleva kokkuleppe olemasolust.

3. Pooled tagavad, et nende füüsilised ja juriidilised isikud, kes saavad salastatud teavet, täidavad käesolevast kokkuleppest tulenevaid kohustusi.

4. Vastuvõttev pool tohib saadud salastatud teavet edastada kolmandatele isikutele ainult päritolupoole eelneval kirjalikul loal.

Artikkel 11. Salastatud lepingutega seotud nõuded

1. Pool, kes soovib sõlmida salastatud lepingut teise poole lepinglasega või volitada oma lepinglast sõlmima teise poole territooriumil salastatud projekti põhjal salastatud lepingut, hangib oma riigi julgeoleku volitatud esindaja kaudu teise poole julgeoleku volitatud esindajalt eelneva kirjaliku kinnituse selle kohta, et asjaomasel lepinglasel on nõuetekohase tasemega juriidilise isiku juurdepääsuluba.

2. Lepinglane kohustub:
a) tagama, et tema ruumid vastavad salastatud teabe käitlemise nõuetele;
b) omama asjakohast juurdepääsuluba;
c) tagama nõuetekohase füüsilise isiku juurdepääsuloa väljastamise isikutele, kellel on seoses oma tööülesannetega vaja juurdepääsu salastatud teabele;
d) tagama, et kõikidele isikutele, kellel on juurdepääs salastatud teabele, tutvustatakse nende salastatud teabe kaitsmise kohustusi riigisiseste õigusaktide kohaselt;
e) julgeolekuinspektsiooni oma ruumides.

3. Alltöövõtja peab täitma samu julgeolekukohustusi kui lepinglane.

4. Riigi julgeoleku volitatud esindaja on pädev tagama, et lepinglane täidab lõikes 2 sätestatud kohustusi.

5. Kui füüsilised või juriidilised isikud, kelle elu- või asukoht on ühe poole territooriumil, ning füüsilised või juriidilised isikud, kelle elu- või asukoht on teise poole territooriumil, alustavad läbirääkimisi salastatud lepingu sõlmimise üle, teatab selle poole julgeoleku volitatud esindaja, kelle territooriumil kõnealust salastatud lepingut täitma hakatakse, teisele poolele selle lepinguga seotud salastatud teabe kõrgeima salastatuse taseme.

6. Poolte füüsiliste või juriidiliste isikute vahel käesoleva kokkuleppe kohaselt sõlmitud salastatud lepingud peavad sisaldama projekti julgeolekueeskirja, milles määratakse:
a) projekti salastamisjuhend ja salastatud teabe loend;
b) teabe salastatuse muutmisest teatamise kord;

c) sidekanalid ja elektroonilised sidevahendid;
d) salastatud materjali vedamise kord;
e) salastatud lepinguga seotud salastatud teabe kaitse kooskõlastamise eest vastutavad asutused;
f) kohustus teatada salastatud teabe ohtusattumisest või sellekohasest kahtlusest.

7. Salastatud lepingu julgeolekueeskirja koopia edastatakse selle poole julgeoleku volitatud esindajale, kelle territooriumil salastatud lepingut täidetakse, et tal oleks võimalik jälgida ja kontrollida julgeolekunõuete täitmist.

8. Poolte julgeoleku volitatud esindajad võivad vastastikuste külastuste põhjal analüüsida lepinglase poolt salastatud lepinguga seotud salastatud teabe kaitseks võetud meetmete tõhusust. Külastusest teatatakse vähemalt kolmkümmend päeva ette.

Artikkel 12. Külastused

1. Poolte kodanike vastastikused külastused, millega kaasneb juurdepääsuvajadus salastatud teabele, võivad toimuda vastuvõtva poole julgeoleku volitatud esindaja eelneval kirjalikul loal.

2. Üks pool lubab teise poole külastusi, millega kaasneb juurdepääsuvajadus salastatud teabele, üksnes juhul, kui:
a) lähetava poole julgeoleku volitatud esindaja või muu pädev asutus on nendele külastajatele väljastanud nõuetekohase füüsilise isiku juurdepääsuloa ning
b) külastajatel on oma riigisiseste õigusaktide kohaselt õigus saada põhjendatud teadmisvajaduse tõttu salastatud teavet või omada sellele juurdepääsu.

3. Lähetava poole julgeoleku volitatud esindaja teatab kavandatavast külastusest vastuvõtva poole julgeoleku volitatud esindajale külastustaotluses, mis peab laekuma vähemalt kolmkümmend päeva enne külastust.

4. Kiireloomulistel juhtudel tuleb külastustaotlus edastada vähemalt seitse päeva varem.

5. Külastustaotlus peab sisaldama järgmist:
a) külastaja ees- ja perekonnanimi, sünniaeg ja -koht, kodakondsus, passi või isikutunnistuse number;
b) selle asutuse nimi, mida külastaja esindab või kus ta töötab;
c) külastatava asutuse nimi ja aadress;
d) tõend külastaja füüsilise isiku juurdepääsuloa olemasolu ja kehtivuse kohta;
e) visiidi või visiitide eesmärk ja otstarve;
f) visiidi või visiitide eeldatav toimumisaeg ja kestus ning kordusvisiitide puhul kogu ajavahemik, mida need hõlmavad;
g) külastatava asutuse kontaktisiku nimi ja telefoninumber, varasemad kontaktid ja muu teave, mis aitab otsustada visiidi või visiitide põhjendatuse üle;
h) kuupäev, allkiri ja riigi julgeoleku volitatud esindaja ametlik pitser.

6. Külastustaotluse adressaadist poole julgeoleku volitatud esindaja vaatab taotluse läbi ja teeb selle rahuldamise kohta otsuse ning teatab otsusest taotluse saatnud poole julgeoleku volitatud esindajale.

7. Kolmandate isikute esindajate külastused, millega kaasneb juurdepääsuvajadus päritolupoole salastatud teabele, on lubatud üksnes päritolupoole julgeoleku volitatud esindaja kirjalikul nõusolekul.

8. Kui külastus on kinnitatud, edastab vastuvõtva poole julgeoleku volitatud esindaja külastustaotluse koopia külastatava asutuse julgeolekutöötajatele.

9. Külastusloa kehtivus ei tohi ületada 12 kuud.

10. Riikide julgeoleku volitatud esindajad võivad iga projekti või lepingu puhul koostada isikute nimekirjad, kellele on lubatud korduskülastused. Nimekirjade esialgne kehtivusaeg on 12 kuud.

11. Kui riikide julgeoleku volitatud esindajad on nimekirjad kinnitanud, kooskõlastatakse konkreetsete külastuste tingimused otse külastatavate asutuste esindajatega, lähtudes käesolevast kokkuleppest.

Artikkel 13. Salastatud teabe ohtusattumine

1. Salastatud teabe kaitse nõuete rikkumise korral, mille tulemusel teise poole koostatud või temalt saadud salastatud teave satub ohtu või on kahtlus, et see on ohtu sattunud, teatab selle poole julgeoleku volitatud esindaja, kelle territooriumil julgeolekunõuete rikkumine toimus või salastatud teave ohtu sattus, teise poole julgeoleku volitatud esindajale juhtunust võimalikult kiiresti ning viib läbi nõuetekohase uurimise.

2. Kui salastatud teabe kaitse nõudeid rikutakse või salastatud teave satub ohtu muudes riikides, võtab salastatud teabe edastanud poole julgeoleku volitatud esindaja lõikes 1 ettenähtud meetmeid.

3. Teine pool võtab vajaduse korral uurimisest osa.

4. Igal juhul teatatakse teisele poolele kirjalikult uurimise tulemustest, sealhulgas salastatud teabe kaitse nõuete rikkumise või salastatud teabe ohtusattumise põhjustest, tekitatud kahju ulatusest ning uurimise järeldustest.

Artikkel 14. Kulud

Kumbki pool kannab oma kokkuleppe täitmisega ja selle järelevalvega seotud kulud.

Artikkel 15. Vaidluste lahendamine

Vaidlused kokkuleppes ettenähtud meetmete tõlgendamise ja kohaldamise üle lahendatakse diplomaatiliste kanalite kaudu.

Artikkel 16. Muudatused

1. Käesolevat kokkulepet võib muuta kummagi poole taotlusel.

2. Muudatused jõustuvad artikli 18 tingimuste kohaselt.

Artikkel 17. Kehtivusaeg ja lõpetamine

1. Kokkulepe sõlmitakse määramata ajaks.

2. Kumbki pool võib kokkuleppe igal ajal lõpetada.

3. Lõpetamisest tuleb teisele poolele teatada kirjalikult diplomaatiliste kanalite kaudu ning leping lõpeb kuus kuud pärast teate kättesaamist.

4. Kokkuleppe lõpetamisest olenemata kaitstakse kokkuleppe alusel saadud teavet edasi selle sätete kohaselt, kuni päritolupool vastuvõtva poole sellest kohustusest vabastab.

Artikkel 18. Jõustumine

1. Pooled teatavad teineteisele kirjalikult diplomaatiliste kanalite kaudu kokkuleppe jõustumiseks vajaliku riigisisese menetluse lõpetamisest.

2. Kokkulepe jõustub kolmekümnendal päeval pärast seda, kui saabub viimane lõikes 1 osutatud teade.

Selle kinnituseks on poolte täievolilised esindajad kokkuleppele alla kirjutanud.

Koostatud Lissabonis 29. novembril 2005 kahes originaaleksemplaris eesti, portugali ja inglise keeles; kõik tekstid on võrdselt autentsed. Kokkuleppe erineva tõlgendamise korral lähtutakse ingliskeelsest variandist.

Eesti Vabariigi nimel	**Portugali Vabariigi nimel**
Heiki Loot	**Fernando Manuel de Mendonça d'Oliveira Neves**
Riigisekretär	**Euroopa asjade riigisekretär**

AGREEMENT ON THE PROTECTION OF CLASSIFIED INFORMATION BETWEEN THE REPUBLIC OF ESTONIA AND THE PORTUGUESE REPUBLIC

The Republic of Estonia and the Portuguese Republic
Hereinafter referred to as the "Parties",

Recognising the need of the Parties to guarantee the protection of the Classified Information exchanged between the Parties, their individuals or legal entities, under cooperation agreements or contracts concluded or to be concluded;

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

Agree as follows:

Article 1. Object

The present Agreement establishes the security rules applicable to all cooperation agreements or contracts, which envisage the transmission of Classified Information, concluded or to be concluded between the competent national authorities of both Parties or by individuals or legal entities duly authorized to that purpose.

Article 2. Scope of application

1. The present Agreement sets out security rules for the protection of Classified Information exchanged between the Parties.

2. The present Agreement is not applicable to direct co-operation between the intelligence services.

Article 3. Definitions

For the purposes of the present Agreement:
a) “Classified Information” designates the information, documents and materials, regardless of their form, nature, and means of transmission, determined to require protection against unauthorised disclosure, which has been so designated by security classification;
b) “National Security Authority” designates the authority designated by a Party as being responsible for the implementation and supervision of the present Agreement;
c) “The Originating Party” designates the Party, which gives or transmits Classified Information to the other Party;
d) “The Receiving Party” designates the Party to which Classified Information is given or transmitted to by the Originating Party;
e) “Third Party” designates any international organisation or state, including its citizens and legal entities, that is not a Party to the present Agreement;
f) “Contractor” designates an individual or a legal entity possessing the legal capacity to conclude contracts;
g) “Classified Contract” designates an arrangement between two or more Contractors creating and defining enforceable rights and obligations between them, which contains or involves Classified Information;
h) “Personnel Security Clearance” designates the determination by the National Security Authority or other competent authority, that an individual is eligible to have access to Classified Information, in accordance with the national law;
i) “Facility Security Clearance” designates the determination by the National Security Authority or other competent authority that, from a security point of view, a legal entity has the physical and organisational capability to use and deposit Classified Information, in accordance with the national law;
j) “Need-to-know” designates that access to Classified Information may only be granted to a person who has a verified requirement for knowledge or possession of such information in order to perform official and professional duties, in accordance with the purpose for which the information was given or transmitted to the Receiving Party;
k) “Project Security Instruction” designates a compilation of security requirements, which are applied to a specific project in order to standardize security procedures;
l) “Project Security Classification Guide” designates the part of the Project Security Instruction, which identifies the elements of the project that are classified and specifies their security classification levels.

Article 4. National Security Authorities

1. The National Security Authorities are:

For the Republic of Estonia
Security Department, Ministry of Defence, Sakala Street 1, 15094 Tallinn, Estonia;

For the Portuguese Republic:
National Security Authority, Presidency of the Council of Ministers, Av. Ilha da Madeira, 1, 1400-204 Lisbon, Portugal.

2. The Parties shall inform each other, through diplomatic channels, of modifications concerning their National Security Authorities.

Article 5. Security principles

1. The protection and use of the Classified Information exchanged between the Parties is ruled by the following principles:
a) The Parties shall afford all transmitted, produced or developed Classified Information the same degree of security protection as is provided for their own Classified Information of the equivalent level;
b) Access to Classified Information is allowed only to persons who have a Need-to-know and, in case of information classified KONFIDENTSIAALNE/ CONFIDENCIAL and above, hold a valid Personnel Security Clearance issued by the competent authorities.

2. In order to achieve and maintain comparable standards of security, the National Security Authorities shall, on request, provide each other with information about their security standards, procedures and practices for protection of Classified Information.

Article 6. Security classification

1. The Parties agree that the following security classification levels are equivalent and correspond to the security classification levels specified in the national law of each Party:

Republic of Estonia	Portuguese Republic	Equivalent in English
TÄIESTI SALAJANE	MUITO SECRETO	TOP SECRET
SALAJANE	SECRETO	SECRET
KONFIDENTSIAALNE	CONFIDENCIAL	CONFIDENTIAL
PIIRATUD	RESERVADO	RESTRICTED

2. The Receiving Party shall mark the received Classified Information with its own equivalent security classification level marking, in accordance with the equivalences referred to in paragraph 1 of the present Article.

3. The Parties shall inform each other about all subsequent classification level alterations to the Classified Information transmitted.

4. The Receiving Party shall neither downgrade nor declassify the received Classified Information without the prior written consent of the Originating Party.

Article 7. Security clearance

1. On request, the Parties, through their National Security Authorities, preceding the issue of the Personnel Security Clearance and the Facility Security Clearance, shall assist each other during the clearance procedures of their individuals or legal entities living or located in the territory of the other Party, taking into account their national law.

2. The Parties shall recognise the Personnel Security Clearance and Facility Security Clearance issued in accordance with the national law of the other Party. The equivalence of the security clearance levels shall be in compliance with Article 6 of the present Agreement.

3. The National Security Authorities shall communicate to each other any information with respect to changes of the related Personnel Security Clearances and Facility Security Clearances, particularly in cases of withdrawal or downgrading of their level.

Article 8. Translation, reproduction and destruction

1. Classified Information marked as SALAJANE/SECRETO or above shall be reproduced and translated only upon the written permission of the National Security Authority of the Originating Party.

2. Translations and reproductions of Classified Information shall be made in accordance with the following procedures:
a) The individuals shall hold the appropriate Personnel Security Clearance as required in Article 5;
b) The translations and the reproductions shall be marked and placed under the same protection as the original information;
c) The translations and the number of reproductions shall be limited to that required for official purposes;
d) The translations shall bear an appropriate note in the language into which it is translated indicating that it contains Classified Information received from the Originating Party.

3. Classified Information marked as TÄIESTI SALAJANE / MUITO SECRETO shall not be destroyed and it shall be returned to the National Security Authority of the Originating Party.

4. Destruction of Classified Information marked as SALAJANE/SECRETO shall be notified to the National Security Authority of the Originating Party.

5. Information classified up to, and including, KONFIDENTSIAALNE/CONFIDENCIAL, shall be destroyed in accordance with the national law.

6. In case of crisis situation, which makes it impossible to protect and return Classified Information generated or transferred according to the present Agreement the Classified Information shall be destroyed immediately. The Receiving Party shall notify the National Security Authority of the Originating Party about the destruction of the Classified Information as soon as possible.

Article 9. Transmission of Classified Information

1. The Classified Information shall be transmitted between the Parties through channels mutually approved by the National Security Authorities.

2. The Parties may transmit Classified Information by electronic means in accordance with security procedures mutually approved by the National Security Authorities.

3. Delivery of large items or quantities of Classified Information shall be approved by both National Security Authorities on a case-by-case basis.

4. The Receiving Party shall confirm in writing the reception of the Classified Information and transmits it to the users.

Article 10. Use and compliance

1. The transmitted Classified Information shall be used only for the purpose that it was transmitted for.

2. Each Party shall inform its individuals and legal entities of the existence of the present Agreement, whenever Classified Information is involved.

3. Each Party shall ensure that all individuals and legal entities, which receive Classified Information, duly comply with the obligations of the present Agreement.

4. The Receiving Party shall not transmit the Classified Information to a Third Party, without prior written authorization of the Originating Party.

Article 11. Requirements for Classified Contracts

1. One Party, wishing to place a Classified Contract with a Contractor of the other Party or wishing to authorise one of its own Contractors to place a Classified Contract in the territory of the other Party, within a classified project, shall obtain, through its National Security Authority, prior written assurance from the National Security Authority of the other Party that the proposed Contractor holds a Facility Security Clearance of an appropriate level.

2. The Contractor commits itself to:
a) Ensure that its premises have adequate conditions for processing Classified Information;
b) Hold an appropriate security clearance;
c) Have an appropriate Personnel Security Clearance granted to persons who perform functions that require access to Classified Information;
d) Ensure that all persons with access to Classified Information are informed of their responsibility towards the protection of Classified Information in accordance with the national law;
e) Allow security inspections of their premises.

3. Any subcontractor must fulfil the same security obligations as the Contractor.

4. The National Security Authority holds the competence to assure the compliance of the Contractor with the commitments set in paragraph 2 of the present Article.

5. As soon as pre-contractual negotiations begin between individuals living, or legal entities located in the territory of one of the Parties and other individuals living, or legal entities located in the other Party’s territory, aiming at the signing of Classified Contracts, the National Security Authority of the Party in whose territory the Classified Contract will be performed shall inform the other Party of the highest security classification level given to the Classified Information related to the contract which is being negotiated.

6. Every Classified Contract signed by individuals or legal entities of the Parties under the present Agreement shall include a Project Security Instruction identifying the following aspects:
a) Project Security Classification Guide and list of Classified Information;
b) Procedure for the communication of changes in the classification of information;
c) Communication channels and means for electronic transmission;
d) Procedure for the transportation of Classified Information;
e) The authorities responsible for the co-ordination of the safeguarding of Classified Information related to the Classified Contract;
f) An obligation to notify any actual or suspected compromise of Classified Information.

7. Copy of the Project Security Instruction of any Classified Contract shall be forwarded to the National Security Authority of the Party in whose territory the Classified Contract is to be performed, in order to allow adequate security supervision and control.

8. Representatives of the National Security Authorities may visit each other in order to analyse the efficiency of the measures adopted by a Contractor for the protection of Classified Information involved in a Classified Contract. Notice of the visit shall be provided, at least, thirty days in advance.

Article 12. Visits

1. Visits entailing access to Classified Information by citizens from one Party to the other Party are subject to prior written authorisation given by the National Security Authority of the host Party.

2. Visits entailing access to Classified Information shall be allowed by one Party to visitors from the other Party, only if they have been:
a) Granted appropriate Personnel Security Clearance by the National Security Authority or other competent authority of the requesting Party; and
b) Authorised to receive or to have access to Classified Information on a Need-to- know basis, in accordance with the national law.

3. The National Security Authority of the requesting Party shall notify the National Security Authority of the host Party of the planned visit through a request for visit, which has to be received at least thirty days before the visit takes place.

4. In urgent cases, the request for visit shall be transmitted at least seven days in advance.

5. The request for visit shall include:
a) Visitor's first and last name, place and date of birth, citizenship, passport or identity card number;
b) Name of the entity, which the visitor represents or to which the visitor belongs;
c) Name and address of the entity to be visited;
d) Certification of the visitor's Personnel Security Clearance and its validity;
e) Objective and purpose of the visit or visits;
f) Expected date and duration of the requested visit or visits, and, in case of recurring visits, the total period covered by the visits;
g) Name and phone number of the point of contact at the entity to be visited, previous contacts and any other information useful to determine the justification of the visit or visits;
h) The date, signature and the official seal of the National Security Authority.

6. The National Security Authority of the Party that receives a request for visit examines and decides on the request and shall inform of its decision the National Security Authority of the requesting Party.

7. Visits of individuals from a Third Party, entailing access to Classified Information of the Originating Party shall only be authorized by a written consent of the National Security Authority of the Originating Party.

8. Once the visit has been approved, the National Security Authority of the host Party shall provide a copy of the request for visit to the security officers of the entity to be visited.

9. The validity of visit authorisation shall not exceed twelve months.

10. For any project or contract the National Security Authorities may agree to establish lists of authorized persons to make recurring visits. Those lists are valid for an initial period of twelve months.

11. Once those lists have been approved by the National Security Authorities, the terms of the specific visits shall be directly arranged with the representatives of the entities to be visited, in accordance with the present Agreement.

Article 13. Compromise of Classified Information

1. In case of breach of security that results in a certain or suspected compromise of Classified Information originated by or received from the other Party, the National Security Authority of the Party where the breach of security or compromise of Classified Information occurs shall inform the National Security Authority of the other Party, as soon as possible, and carry out the appropriate investigation.

2. If a breach of security or compromise of Classified Information occurs in a state other than the Parties, the National Security Authority of the transmitting Party shall take the actions prescribed in paragraph 1 of the present Article.

3. The other Party shall, if required, co-operate in the investigation.

4. In any case, the other Party shall be informed of the results of the investigation, in writing, including the reasons for the breach of security or compromise of Classified Information, the extent of the damage and the conclusions of the investigation.

Article 14. Expenses

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

Article 15. Settlement of Disputes

Any dispute concerning the interpretation or application of the measures prescribed in the present Agreement shall be settled through diplomatic channels.

Article 16. Amendments

1. The present Agreement may be amended on request of one of the Parties.

2. The amendments shall enter into force in accordance with the terms specified in Article 18 of the present Agreement.

Article 17. Duration and Termination

1. The present Agreement shall remain in force for an indeterminate period of time.

2. Each Party may at any time terminate the present Agreement.

3. The termination shall be notified to the other Party, in writing and through diplomatic channels, producing its effects six months after the date of reception of the notification.

4. Notwithstanding the termination, all Classified Information transferred pursuant to the present Agreement shall continue to be protected in accordance with the provisions set forth herein, until the Originating Party dispenses the Receiving Party from this obligation.

Article 18. Entry into force

1. The Parties shall notify each other, in writing and through diplomatic channels, that all internal procedures necessary for bringing the Agreement into force have been fulfilled.

2. The present Agreement shall enter into force on the thirtieth day following the receipt of the last of the notifications referred to in paragraph 1 of the present Article.

In witness thereof, the undersigned, duly authorized, have signed the present Agreement.

Done at Lisbon, on 29 November 2005 in two originals, each one in the Estonian, Portuguese and English languages, each text being equally authentic. In case of any divergence of interpretation the English text shall prevail.

For the Republic of Estonia	**For the Portuguese Republic**
Heiki Loot	**Fernando Manuel de Mendonça d'Oliveira Neves**
(Secretary of State)	**(Secretary of State for European Affaires)**