Väljaandja:	Vabariigi Valitsus
Akti liik:	välisleping
Teksti liik:	algtekst
Jõustumise kp:	04.02.2004
Avaldamismärge:	RT II 2004, 4, 9

Eesti Vabariigi valitsuse ning Suurbritannia ja Põhja-Iiri Ühendkuningriigi valitsuse salastatud kaitsealase teabe kaitse vastastikuse mõistmise memorandum

(õ)9.04.10 12:25

Vabariigi Valitsuse 11.12.2003 korraldus nr 814 memorandumi eelnõu heakskiitmise kohta

Välisministeeriumi teadaanne välislepingu jõustumise kohta

Eesti Vabariigi valitsuse ning Suurbritannia ja Põhja-Iiri Ühendkuningriigi valitsuse salastatud kaitsealase teabe kaitse vastastikuse mõistmise memorandumi muutmise kokkulepe

Välisministeeriumi teadaanne välislepingu lõppemise kohta

Eesti Vabariigi ning Suurbritannia ja Põhja-Iiri Ühendkuningriigi salastatud teabe kaitse kokkulepe

Alla kirjutatud 4. veebruaril 2004. a Tallinnas, jõustunud 4. veebruaril 2004. a

SISSEJUHATUS

Eesti Vabariigi valitsus ning Suurbritannia ja Põhja-Iiri Ühendkuningriigi valitsus, edaspidi *lepingupooled*,

soovides kaitsta teineteisele ning kummagi kaubandus- ja tööstusorganisatsioonidele edastatud kaitsekoostöö, teadustöö, tootmise ning hanketegevuse alast salastatud teavet,

on oma riigi julgeoleku huvides kokku leppinud järgmises.

Artikkel 1. Eesmärgid ja kehtivusala

1. Memorandum on aluseks kõikidele lepingupoolte vahelistele ettevõtmistele ja kokkulepetele, mis on seotud järgmise salastatud teabega:
a. lepingupoolte riigikaitse-, julgeoleku- või muu kaitsealane koostöö;
b. lepingupoolte juriidiliste isikute või eraettevõtete riigikaitse-, julgeoleku- või muu kaitsealane koostöö, teabevahetus, ühisettevõte, leping või muu suhe;
c. lepingupoole kaitsealase seadmestiku, tehnoloogia ja tehnoloogilise teabe müük teisele lepingupoolele;
d. lepingupoolte esindajate, töötajate või nõustajate (eraisik või muu) vahel edastatav riigikaitse-, julgeoleku- või muu kaitsealane teave.

2. Lepingupool ei või memorandumile tuginedes nõuda salastatud teavet, mille teine lepingupool on saanud kolmandalt isikult.

3. Memorandumiga ei reguleerita luurealase ja massihävitusrelvi käsitleva teabe vahetamist.

Artikkel 2. Mõisted

1. Memorandumis kasutatakse järgmisi mõisteid, millel on järgmine tähendus:
a. «salastatud teave»:
i) mis tahes salajane asi, milleks võib olla salastatud teabe suuline või visuaalne edastamine, salastatud sõnumi sidevahendite või elektroonilisel teel edastamine või allpool määratletud materjal;
ii) «materjal» hõlmab kõiki allpool määratletud dokumente ning kõiki valminud või tootmises olevaid masinaid, seadmeid, relvi või relvasüsteeme;
iii) «dokument» on mis tahes vormis salvestatud teave, olenemata teabekandjast;
b. «leping» on kahe või enama lepinglase kokkulepe, millega määratakse kindlaks nende õigused ja kohustused;

c. «salastatud leping» on salastatud teavet sisaldav või sellega seotud kokkulepe;
d. «lepinglane» on füüsiline või juriidiline isik, kellel on õigus sõlmida lepinguid;
e. «julgeolekut käsitlevate õigusaktide rikkumine» on riigi julgeolekut käsitlevate õigusaktidega vastuolus olev tegu või tegevusetus, mille tõttu võib tekkida salastatud teabe lekkimise oht või leke;
f. «teabeleke» on olukord, kus salastatud teave või selle osa on muutunud või võib muutuda kättesaadavaks isikule, asutusele, ettevõttele või riigile, kellel ei ole teabele juurdepääsu luba või volitust;
g. «juurdepääsuluba» on julgeolekukontrolli läbinud isikule või asutusele- ettevõttele antud õigus riigi õigusaktide kohaselt pääseda ligi kindlaksmääratud salastustasemega teabele ja seda töödelda;
h. «julgeoleku kinnitus» on pädeva asutuse väljastatud teade selle kohta, et salastatud teavet kaitstakse riigi julgeolekut käsitlevate õigusaktide kohaselt, või et isikule või asutusele-ettevõttele on väljastatud juurdepääsuluba;
i. «pädev asutus» on memorandumi artiklis 3 nimetatud asutus;
j. «teadmisvajadus» on isiku põhjendatud tarvidus saada ametikohustuste täitmiseks salastatud teavet lepingupoolte teabe edastamise tingimuste kohaselt;
k. «teabe edastaja» on lepingupool, kes edastab salastatud teavet ja keda esindab pädev asutus;
l. «teabe vastuvõtja» on lepingupool, kellele salajane teave edastatakse ja keda esindab pädev asutus.

2. Lepingupooled kasutavad memorandumis järgmisi salastustasemeid ja nende vasteid:

Eesti Vabariik	Ühendkuningriik
SALAJANE	SECRET
KONFIDENTSIAALNE	CONFIDENTIAL
PIIRATUD	RESTRICTED

Artikkel 3. Pädevad asutused

1. Kokkuleppe rakendamise ja järelevalve eest vastutavad pädevad asutused on:

a. *Eesti Vabariigis*:
Riigi julgeoleku volitatud esindaja
Riigisaladuse kaitse osakonna juhataja; Kaitseministeerium, Sakala 1, 15094 Tallinn, Eesti;

b. *Ühendkuningriigis*:
Kaitseministeeriumit puudutavates küsimustes ja tööstusliku julgeoleku poliitika alal:
Director of Defence Security, St Giles Court, 1-13 St Giles High Street, London WC2H 8LD, England;
Julgeolekumeetmete rakendamise alal:
Defence Procurement Agency (FMG 2), Abbey Wood, Bristol, BS34 8JH, England.

Artikkel 4. Kasutamise ja avalikustamise piirangud

1. Teabe vastuvõtjal on lubatud avalikustada või kasutada või anda luba avalikustada või kasutada salastatud teavet eesmärkidel ja ulatuses, mille on kindlaks määranud teabe edastaja või tema esindaja.

2. Teabe vastuvõtja ei edasta memorandumi kohaselt saadud salajast teavet riigiametnikule, lepinglasele, lepinglase töötajale, kolmanda riigi kodanikule või rahvusvahelisele organisatsioonile ega avalikusta sellist teavet ilma teabe edastaja eelneva kirjaliku loata.

Artikkel 5. Salastatud teabe kaitse

1. Teabe edastaja kohustub:
a. informeerima teabe vastuvõtjat teabe salastatusest ja kõikidest selle avalikustamise tingimustest või kasutuspiirangutest;
b. märgistama dokumendid asjakohaselt ning
c. informeerima teabe vastuvõtjat salastustaseme hilisemast muutmisest.

2. Teabe vastuvõtja kohustub oma riigi seaduste ja muude õigusaktide kohaselt:
a. kaitsma salastatud teavet võrdväärselt riigi salastatud teabega vastavalt memorandumi artikli 2 lõikes 2 loetletud salastustasemetele;
b. märgistama salastatud teave (sealhulgas tõlked ja koopiad) võrdväärselt riigi salastustasemega memorandumi artikli 2 lõike 2 kohaselt;
c. tagama, et salastustaset ei muudeta, välja arvatud teabe edastaja poolt või nimel antud kirjalikul loal.

3. Et luua ja rakendada võrreldavaid julgeolekut käsitlevaid õigusakte, teatab pädev asutus asjakohase taotluse korral teisele pädevale asutusele oma riigi salastatud teavet käsitlevad julgeolekut käsitlevad õigusaktid, toimingud ja korra ning võimaldab teise pädeva asutuse esindajatel külastada sel eesmärgil oma asutust. Kui lepingupool muudab oma julgeolekut käsitlevaid õigusakte oluliselt leebemaks, peab ta sellest teatama teisele lepingupoolele.

Artikkel 6. Salastatud teabele juurdepääs

Salastatud teabele pääsevad ligi üksnes isikud, kellel on teadmisvajadus ja kellele teabe vastuvõtja pädev asutus on riigi õigusaktide kohaselt andnud juurdepääsuõiguse kindlaksmääratud salastustasemega teabele.

Artikkel 7. Salastatud teabe edastamine

1. Lepingupooled vahetavad salastatud teavet vastavalt teabe edastaja julgeolekut käsitlevatele õigusaktidele. *CONFIDENTIAL*või *SECRET*ja KONFIDENTSIAALNE või SALAJANE teave edastatakse tavaliselt diplomaatiliste kanalite kaudu, kuid seda võib edastada ka muul viisil, kui mõlema lepingupoole pädev asutus annab selleks oma eelneva nõusoleku.

2. Kui on vaja edastada suuri esemeid või suurt hulka salastatud teavet, otsustavad ja kinnitavad pädevad asutused ühiselt nende edastamise viisi.

3. *RESTRICTED*ja PIIRATUD tasemega salastatud teavet vahetatakse teabe edastaja julgeolekut käsitlevate õigusaktide kohaselt. Kui *RESTRICTED*tasemega salastatud teavet edastatakse esimest korda Eesti lepinglasele, kellel ei ole asutuse-ettevõtte juurdepääsuluba, edastatakse teave pädeva asutuse kaudu.

Artikkel 8. Külastused

1. Külalised, sealhulgas teisest riigist ametilähetuses viibivad külalised, vajavad juurdepääsuks salastatud teabele või sissepääsuks salastatud kaitsetööga tegelevate asutuste või lepinglaste territooriumile vastuvõtva riigi pädeva asutuse eelnevat nõusolekut. Külastustaotlused esitatakse suursaatkondade kaudu.

2. Kõik külalised peavad järgima vastuvõtva riigi julgeolekut käsitlevaid õigusakte.

3. Konkreetse projekti või lepingu korral võib mõlema lepingupoole nõusolekul kehtestada korduvkülaliste nimekirja. Selle esialgne kehtivusaeg ei ületa 12 kuud ning seda võib pädevate asutuste eelneva nõusoleku korral pikendada (mitte rohkem kui 12 kuud korraga). Nimekiri esitatakse teabe vastuvõtja tavapärase korra kohaselt. Pärast nimekirja kinnitamist võivad asjaomased asutused või ettevõtted korraldada ise nimekirjas loetletud isikute külastusi.

4. Teavet, mida külalistele antakse või mida nad teada saavad, käsitatakse memorandumi kohaselt edastatud teabena.

5. Külalist saatev pädev asutus teatab vastuvõtva lepingupoole pädevale asutusele kavatsetavast külastusest vähemalt kolm nädalat ette. Erivajaduse korral antakse külalisele eelnevalt kooskõlastatud juurdepääsuluba niipea kui võimalik.

6. Külastustaotluses esitatakse vähemalt järgmised andmed:
a. külastaja nimi, sünniaeg ja -koht, kodakondsus ja passi number;
b. külastaja ametinimetus ja esindatava asutuse, ettevõtte või organisatsiooni nimi;
c. külastajale tema riigi pädeva asutuse antud juurdepääsuluba;
d. külastuse kuupäevad;
e. külastuse eesmärk;
f. külastatava asutuse, ettevõtte või organisatsiooni nimi;
g. vastuvõtvas riigis külastatavate isikute nimed.

Artikkel 9. Lepingud

1. Kui lepingupool kavatseb sõlmida või volitada oma riigi lepinglast sõlmima teise riigi lepinglasega lepingut, mis on seotud *CONFIDENTIAL*või *SECRET*ehk KONFIDENTSIAALSE või SALAJASE tasemega salastatud teabega, siis peab teabe edastaja saama teabe vastuvõtja pädevalt asutuselt eelnevalt kirjaliku kinnituse selle kohta, et väljapakutud lepinglasel on vajaliku tasemega juurdepääsuluba ja vahendid kaitsta sellise tasemega salastatud teavet. Kinnitusega võetakse vastutus selle eest, et juurdepääsu omav lepinglane töötleb salastatud teavet riigi julgeolekut käsitlevate õigusaktide kohaselt ja on pädeva asutuse järelevalve all.

2. Lepingud, mis on sõlmitud pärast sellist järelepärimist, sisaldavad vähemalt järgmistest sätetest koosnevat julgeolekunõuete klauslit:
a. «salastatud teabe» ning kahe lepingupoole võrdväärsete salastustasemete määratlus memorandumi kohaselt;
b. mõlema lepingupoole pädeva asutuse nimi, kes lubab edastada lepinguga seotud salastatud teavet ning koordineerib selle kaitsmist;
c. pädevate asutuste ja lepinglaste vahelised salastatud teabe edastamise kanalid;
d. võimalikest muudatustest teatamise toimimisviisid, kui muutub salastatud teabe salastustase või kui teavet pole enam vaja kaitsta;
e. lepingupoole personali külastuste, juurdepääsu ja inspektsiooni lubamise kord teise lepingupoole riigis asuvatesse ettevõtetesse.

3. Teabe edastaja pädev asutus edastab teabe vastuvõtja pädevale asutusele salastatud lepingu oluliste osade koopia memorandumi artiklis 3 osutatud aadressil, et tagada asjakohane julgeoleku järelevalve.

4. Lepingu juures on lisa, mis sisaldab lepingu iga aspekti julgeolekunõuete ja salastatuse juhist. Ühendkuningriigis paigutatakse juhis julgeolekuklauslitesse ja lepingu julgeolekuosasse. Eesti Vabariigis paigutatakse see lepingu julgeolekuklauslitesse. Juhises määratakse kõik lepingu salastatud aspektid või lepingu täitmise käigus tekkivad salastatud aspektid ning määratakse nende salastustase. Nõuete või aspektide muudatustest teatatakse vajaduse korral ning teabe edastaja teatab teabe vastuvõtjale kogu teabe avalikuks muutmisest.

Artikkel 10. Tööstusliku julgeoleku vastastikused meetmed

1. Pädev asutus teatab teise lepingupoole taotluse korral oma riigis asuva ettevõtte julgeoleku staatusest. Pädev asutus teatab teise lepingupoole taotluse korral ka oma riigi kodaniku juurdepääsuloa staatuse. Neid teateid nimetatakse asutuste-ettevõtete või isikute vastastikusteks juurdepääsulubadeks.

2. Taotluse korral teeb pädev asutus kindlaks, kas päringu objektiks oleval ettevõttel või isikul on juurdepääsuluba, ning kui luba on olemas, edastab selle kohta kinnituse. Kui ettevõttel või isikul ei ole juurdepääsuluba või kui see on antud nõutust madalama tasemega teabe jaoks, saadetakse teade, et juurdepääsuloa kinnitust ei ole võimalik kohe väljastada, kuid taotlust menetletakse. Pärast järelepärimist väljastatud juurdepääsuloa kohta saadetakse kinnitus.

3. Ettevõttele, kes registrijärgse asukohariigi pädeva asutuse hinnangul on kolmanda riigi omandis või selle juhtimise või mõju all, mille eesmärgid ei lange kokku asukohariigi eesmärkidega, ei väljastata juurdepääsuluba ning sellest teatatakse taotluse esitanud pädevale asutusele.

4. Kui pädev asutus saab negatiivset teavet isikust, kelle kohta on välja antud juurdepääsuloa kinnitus, teatab ta teisele pädevale asutusele selle teabe sisu ja meetmed, mida ta on võtnud või kavatseb võtta. Mõlemad pädevad asutused võivad taotleda teise pädeva asutuse varem väljastatud isiku juurdepääsuloa läbivaatamist, kui taotlusele on lisatud põhjendus. Taotluse esitanud pädevale asutusele teatatakse läbivaatamise tulemused ja võimalikud järgnevad meetmed.

5. Teabe, mis seab kahtluse alla vastastikuse juurdepääsuloa saanud ettevõtte sobivuse pääseda juurde teise riigi salastatud teabele, üksikasjad edastatakse viivitamata pädevale asutusele uurimiseks.

6. Kui pädev asutus peatab isiku juurdepääsuloa, võtab meetmed selle tühistamiseks, peatab teise riigi kodanikule juurdepääsuloa alusel võimaldatud juurdepääsu või võtab meetmed selle lõpetamiseks, peab ta sellest teatama teisele lepingupoolele ja esitama põhjenduse.

7. Kumbki pädev asutus võib taotleda teiselt pädevalt asutuselt mis tahes ettevõttele väljastatud juurdepääsuloa taasläbivaatamist, kui taotlusele on lisatud põhjendus läbivaatamise vajalikkuse kohta. Taotluse esitanud pädevale asutusele teatatakse läbivaatamise tulemused ja otsuse asjaolud.

Artikkel 11. Teabe kadumine või leke

1. Julgeolekut käsitlevate õigusaktide rikkumise korral, mille tõttu kaob teiselt lepingupoolelt pärinev salastatud teave või saavad kahjustada kahe lepingupoole ühised huvid, samuti teabe kõrvalistele isikutele lekitamise kahtluse korral, teatab selle riigi pädev asutus, kus rikkumine aset leidis, sellest viivitamata teise lepingupoole pädevale asutusele.

2. Lepingupool, kelle riigis rikkumine aset leidis või võib aset leida, viib viivitamata läbi uurimise, millele vajaduse korral aitab kaasa teine lepingupool. Igal juhul teatatakse teisele lepingupoolele esimesel võimalusel uurimise tulemused ning võimaluse korral ka julgeolekut käsitlevate õigusaktide rikkumise või teabe lekke põhjused ja ulatuse ning võetud meetmed.

Artikkel 12. Kulud

Kumbki lepingupool kannab kulud, mis tal tekivad seoses memorandumi täitmisega.

Artikkel 13. Muutmine

Memorandumit võib igal ajal muuta lepingupoolte vastastikuse kirjaliku nõusoleku korral.

Artikkel 14. Vaidluste lahendamine

Lepingupooled lahendavad memorandumi tõlgendamise või kohaldamise vaidluse konsultatsioonide teel. Vaidlust ei anta lahendada lepingupoole kohtule, rahvusvahelisele kohtule või kolmandale isikule.

Artikkel 15. Jõustumine ja lõpetamine

1. Memorandum jõustub allkirjastamise päeval ja on jõus seni, kuni seda ei ole lõpetatud vastastikusel kokkuleppel või ühe lepingupoole poolt, kes teatab sellest teisele lepingupoolele kuus kuud kirjalikult ette.

Memorandumi lõpetamise korral on kumbki lepingupool kohustatud esimesel võimalusel salastatud teabe teisele lepingupoolele tagastama või kaitsma seda edasi memorandumi kohaselt.

2. Lepingupooled vaatavad memorandumi ühiselt läbi kümne aasta möödudes selle jõustumise kuupäevast.

Memorandum kajastab Eesti Vabariigi valitsuse ning Suurbritannia ja Põhja- Iiri Ühendkuningriigi valitsuse vahel saavutatud teineteise mõistmist kirjeldatud valdkonnas.

Memorandum on koostatud kahes eksemplaris eesti ja inglise keeles ning alla kirjutatud 4. veebruaril 2004. aastal Tallinnas; mõlemad tekstid on võrdselt autentsed.

Eesti Vabariigi valitsuse nimel	**Suurbritannia ja Põhja-Iiri Ühendkuningriigi valitsuse nimel**
Margus HANSON	**Nigel HAYWOOD**

MEMORANDUM OF UNDERSTANDING BETWEEN THE GOVERNMENT OF THE REPUBLIC OF ESTONIA AND THE GOVERNMENT OF THE UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND CONCERNING THE PROTECTION OF CLASSIFIED DEFENCE INFORMATION

INTRODUCTION

The Government of the Republic of Estonia and the Government of the United Kingdom of Great Britain and Northern Ireland, hereinafter referred to as the Participants;

Wishing to ensure the protection of classified information transferred for the purposes of defence co-operation, research, production and procurement between them or to commercial and industrial organisations in either of the two countries;

Have, in the interests of national security, established the following arrangements:

Section 1 – Objectives and Scope

1. This Memorandum will form the basis of any arrangements involving the transfer of classified information which may be made between the Participants concerning the following subjects:
a. co-operation between the two Participants concerning national defence, security or other defence-related issues;
b. co-operation, exchange of information, joint ventures, contracts or any other relations between entities or private companies in the Participants' countries concerning national defence, security or other defence- related issues;
c. sale of equipment, technology and technology information relating to defence by one Participant to the other;
d. information transferred between the Participants by any representative, employee or consultant (private or otherwise) concerning national defence, security or other defence-related issues.

2. This Memorandum may not be invoked by either Participant to obtain classified information which the other Participant has received from a third party.

3. This Memorandum does not cover the exchange of intelligence information or information relating to weapons of mass destruction.

Section 2 – Definitions

1. For the purposes of this Memorandum the following definitions will apply:
a. "classified information" means:
(i) any classified item, be it an oral or visual communication of classified contents or the electrical or electronic transmission of a classified message, or be it material as defined below;
(ii) "material" includes any document as defined below, and any item of machinery, equipment, weapon or weapon system either manufactured or in the process of manufacture;
(iii) "document" means any form of recorded information regardless of the type of recording medium;
b. "contract" means an agreement between two or more parties creating and defining enforceable rights and obligations between them;
c. "classified contract" means a contract which contains or involves classified information;
d. "contractor" means an individual or legal entity possessing the legal capability to undertake contracts;

e. “breach of security” means an act or omission contrary to national security regulations, the result of which may be to endanger or compromise classified information;
f. “security compromise” means that classified information is compromised because knowledge of it has, in whole or in part, passed to persons or entities or countries without appropriate security clearance or authority to have such access, or because it has been subject to a risk of such passing;
g. “security clearance” means a positive determination following an investigative procedure to ascertain the suitability of a person or entity to have access to and to handle classified information on a certain level in accordance with the respective national security regulations;
h. “security assurance” means a statement issued by the Competent Security Authority declaring that classified information will be protected in accordance with its national security regulations or that individuals or facilities have been granted a personal or facility security clearance;
i. “Competent Security Authority” means an authority specified in Section 3 of this Memorandum;
j. “need to know” means that access to classified information may be granted only if the person requiring it has a verified need to know in connection with his or her official duties, within the framework of which the information was released to the receiving Participant;
k. “originating Participant” means the Participant initiating the classified information, as represented by its Competent Security Authority;
l. “recipient Participant” means the Participant to which the classified information is transmitted, as represented by its Competent Security Authority.

2. The security classifications used by the Participants for the purposes of this Memorandum, with their equivalents, are as follows:

Republic of Estonia	**United Kingdom**
SALAJANE	SECRET
KONFIDENTSIAALNE	CONFIDENTIAL
PIIRATUD	RESTRICTED

Section 3 – Competent Security Authorities

The security authorities responsible for the policy, implementation and supervision of all aspects of this Memorandum in each country are:

a. *for the Republic of Estonia*:
National Security Authority
Director of the Security Department, Ministry of Defence, Sakala 1, 15094 Tallinn, Estonia;

b. *for the United Kingdom*:
Ministry of Defence and industrial security policy:
Director of Defence Security, St Giles Court, 1-13 St Giles High Street, London, WC2H 8LD, England;
Security implementation:
Defence Procurement Agency (FMG 2), Abbey Wood, Bristol, BS34 8JH, England.

Section 4 – Restrictions on Use and Disclosure

1. Unless express consent is given to the contrary, the recipient Participant will not disclose or use, or permit the disclosure or use of, any classified information except for purposes and within any limitations stated by or on behalf of the originating Participant.

2. The recipient Participant will not pass to a Government official, contractor, contractor’s employee or any other person holding the nationality of any third country, or to any international organisation, any classified information supplied under the provisions of this Memorandum, nor will it publicly disclose any such information without the prior written permission of the originating Participant.

Section 5 – Protection of Classified Information

1. The originating Participant will ensure:
a. that the recipient Participant is informed of the classification of the information and of any conditions of release or limitations on its use;
b. that documents are so marked; and
c. that the recipient Participant is informed of any subsequent change in classification.

2. The recipient Participant will, in accordance with its national laws and regulations:
a. afford the same degree of security protection to classified information as is afforded to national classified information of an equivalent classification originated by the recipient Participant in accordance with the security classifications listed in Section 2(2) of this Memorandum;
b. ensure that classified information (including translations and reproductions) is marked with its own equivalent classification in accordance with Section 2(2) of this Memorandum;
c. ensure that classifications are not altered, except as authorised in writing by or on behalf of the originating Participant.

3. In order to achieve and maintain comparable standards of security, each Competent Security Authority will, on request, provide to the other information about its security standards, procedures and practices for safeguarding classified information, and will for this purpose facilitate visits by representatives of the other Competent Security Authority. In the event that either Participant significantly lowers its security standards it will notify the other Participant.

Section 6 – Access to Classified Information

Access to classified information will be limited to those persons who have a need to know, and who have been granted an appropriate security clearance by the recipient Participant's Competent Security Authority, in accordance with its national standards, to the level appropriate to the classification of the information to be accessed.

Section 7 – Transmission of Classified Information

1. Classified information will be transmitted between the Participants in accordance with the national security regulations of the originating Participant. The normal route for information at the CONFIDENTIAL or SECRET and the *KONFIDENTSIAALNE*or *SALAJANE*levels will be through diplomatic channels, but other arrangements may be made if approved in advance by the Competent Security Authorities of both Participants.

2. If the transfer of large items or large quantities of classified information is required, the Competent Security Authorities will jointly decide on and approve the means of transportation.

3. The transmission of classified information at the RESTRICTED and the *PIIRATUD*levels will be in accordance with the national security regulations of the Participant sending the information. In the first instance when RESTRICTED information is to be transmitted to Estonian contractors who do not hold a Facility Security Clearance, it will be sent via the Competent Security Authority.

Section 8 – Visits

1. The prior approval of the Competent Security Authority of the host country will be required in respect of visitors, including those on detached duty from the other country, where access to classified information or to defence establishments or defence contractors' premises engaged in classified work is necessary. Requests for such visits will be submitted through the respective Embassies.

2. All visitors will comply with the security regulations of the host country.

3. In cases involving a specific project or a particular contract it may, subject to the approval of both Participants, be possible to establish Recurring Visitors Lists. These lists will be valid for an initial period not exceeding 12 months and may be extended for further periods (not to exceed 12 months at one time) subject to the prior approval of the Competent Security Authorities. They should be submitted in accordance with the normal procedures of the recipient Participant. Once a list has been approved, visit arrangements may be made direct between the establishments or companies involved in respect of listed individuals.

4. Any information which may be provided to visiting personnel, or which may come to the notice of visiting personnel, will be treated by them as if such information has been furnished pursuant to the provisions of this Memorandum.

5. The Competent Security Authority of the Participant sending the visitor will notify the Competent Security Authority of the Participant receiving the visitor of the visit at least three weeks prior to the planned visit. In case of special needs, security approval of the visit will be granted as soon as possible, subject to prior co-ordination.

6. Visit applications will include at least the following information:
a. name of visitor, date and place of birth, nationality, and passport number;
b. official title of the visitor and the name of the establishment, company or organisation which he represents;
c. security clearance of the visitor as granted by his Competent Security Authority;
d. dates of visit;
e. purpose of visit;
f. name of the establishment, company or organisation to be visited;
g. names of persons to be visited in the host country.

Section 9 – Contracts

1. When proposing to place, or to authorise a contractor in its own country to place, a contract involving information classified at the CONFIDENTIAL or SECRET and the *KONFIDENTSIAALNE*or *SALAJANE*levels with a contractor in the other country, the originating Participant will obtain prior written assurance from the Competent Security Authority of the other Participant that the proposed contractor holds a security clearance

to the appropriate level and also has suitable security facilities to provide adequate protection for classified information of the level concerned. The assurance will carry a responsibility that the security conduct by the cleared contractor will be in accordance with national security rules and regulations and that it will be monitored by his Competent Security Authority.

2. Contracts placed as a consequence of these pre-contract enquiries will contain a security requirement clause incorporating at least the following provisions:
a. the definition of the term “classified information” and of the equivalent levels of security classification of the two Participants in accordance with the provisions of this Memorandum;
b. the names of the Competent Security Authority of each of the two Participants empowered to authorise the release and to co-ordinate the safeguarding of classified information related to the contract;
c. the channels to be used for the transfer of the classified information between the Competent Security Authorities and contractors involved;
d. the procedures and mechanisms for communicating the changes that may arise in respect of classified information either because of changes in its security classification or because protection is no longer necessary;
e. the procedures for the approval of visits, access or inspection by personnel of one Participant to companies in the other Participant’s country which are covered by the contract.

3. The Competent Security Authority of the originating Participant will pass a copy of the relevant parts of the classified contract to the Competent Security Authority of the recipient Participant, at the address shown in Section 3 of this Memorandum, to allow adequate security monitoring.

4. Each contract will contain a supplement or annex providing guidance on the security requirements and on the classification of each aspect or element of the contract. In the United Kingdom the guidance will be contained in specific security clauses and in a Security Aspects Letter (SAL). In the Republic of Estonia this guidance will be set out in the specific security clauses in the contract. The guidance must identify each classified aspect of the contract, or any classified aspect which is to be generated by the contract, and allocate to it a specific security classification. Changes in the requirements or to the aspects or elements will be notified as and when necessary and the originating Participant will notify the recipient Participant when all the information has been declassified.

Section 10 – Reciprocal Industrial Security Arrangements

1. Each Competent Security Authority will notify the security status of a company site in its own country when requested by the other Participant. Each Competent Security Authority will also notify the security clearance status of one of its nationals when so requested. These notifications will be known as reciprocal Facility Security Clearances (FSC) and reciprocal Personnel Security Clearances (PSC) respectively.

2. When requested, the Competent Security Authority will establish the security clearance status of the company or individual which is the subject of the enquiry and forward a security clearance assurance if the company or individual is already cleared. If the company or individual does not have a security clearance, or the clearance is at a lower security level than that which has been requested, notification will be sent that the security clearance assurance cannot be issued immediately, but that action is being taken to process the request. Following successful enquiries an assurance of FSC/PSC will be provided.

3. A company which is deemed by the Competent Security Authority in the country in which it is registered to be under the ownership, control or influence of a third country whose aims are not compatible with those of the host country is not eligible for a FSC and the requesting Competent Security Authority will be notified.

4. If either Competent Security Authority learns of any derogatory information about an individual for whom a PSC assurance has been issued, it will notify the other Competent Security Authority of the nature of the information and the action it intends to take, or has taken. Either Competent Security Authority may request a review of any PSC which has been furnished earlier by the other Competent Security Authority, provided that the request is accompanied by a reason. The requesting Competent Security Authority will be notified of the results of the review and any subsequent action.

5. If information becomes available which raises doubts about the suitability of a reciprocally cleared company to continue to have access to classified information in the other country then details of this information will be promptly notified to the Competent Security Authority to allow an investigation to be carried out.

6. If either Competent Security Authority suspends or takes action to revoke a reciprocal PSC, or suspends or takes action to revoke access which is granted to a national of the other country based upon a security clearance, the other Participant will be notified and given the reasons for such an action.

7. Either Competent Security Authority may request the other to review any company FSC, provided that their request is accompanied by the reasons for seeking the review. Following the review, the requesting Competent Security Authority will be notified of the results and will be provided with facts supporting any decisions taken.

Section 11 – Loss or Compromise

1. In the event of a breach of security involving the loss of classified information originating from the other Participant or affecting the joint interests of the two Participants, or in the event of suspicion that such

information may have been disclosed to unauthorised persons, the Competent Security Authority in whose country the compromise occurs will immediately inform the other Participant's Competent Security Authority.

2. An immediate investigation will be carried out by the Participant in whose country the security compromise has occurred, or is believed to have occurred, if necessary with the co-operation of the other Participant. In any event, that Participant will be informed as soon as practicable of the result of the investigation, including if possible the reasons for and extent of any security breach or compromise, and of any measures taken as a consequence.

Section 12 – Costs

Each Participant will be responsible for any costs which it may incur in the implementation of this Memorandum.

Section 13 – Amendment

This Memorandum may be reviewed or amended at any time with the mutual written consent of the Participants.

Section 14 – Settlement of Disputes

Any dispute regarding the interpretation or application of this Memorandum will be resolved by consultation between the Participants and will not be referred to any national or international tribunal or third party for settlement.

Section 15 – Commencement and Termination

1. This Memorandum will enter into effect on the date of signature and will continue in effect unless terminated either by mutual consent or by either Participant giving six months' notice in writing to the other. In the event of termination each Participant will be responsible either for returning classified information to the other Participant as soon as practicable or for continuing to protect such information in accordance with the provisions of this Memorandum.

2. This Memorandum will be reviewed jointly by the Participants ten years after its effective date.

The foregoing represents the understandings reached between the Government of the Republic of Estonia and the Government of the United Kingdom of Great Britain and Northern Ireland upon the matters referred to therein.

Signed in Tallinn on February 4, 2004 in duplicate in the Estonian and English languages, both texts having equal validity.

For the Government of the Republic of Estonia	**For the Government of the United Kingdom of Great Britain and Northern Ireland**
Margus HANSON	**Nigel HAYWOOD**

Õiend
Metaandmetes parandatud akti andja: Vabariigi Valitsus.