Väljaandja:	Vabariigi Valitsus
Akti liik:	välisleping
Teksti liik:	algtekst
Jõustumise kp:	01.06.2009
Avaldamismärge:	RT II 2009, 16, 43

Eesti Vabariigi valitsuse ja Makedoonia Vabariigi valitsuse salastatud teabe vahetamise ja vastastikuse kaitse kokkulepe

„Eesti Vabariigi valitsuse ja Makedoonia Vabariigi valitsuse salastatud teabe vahetamise ja vastastikuse kaitse kokkuleppe" eelnõu heakskiitmine

Teadaanne riigi julgeoleku volitatud esindaja muutmisest

Teadaanne välislepingu jõustumise kohta

20. novembril 2008. aastal Skopjes, jõustub 1. juunil 2009. a

Eesti Vabariigi valitsus ja Makedoonia Vabariigi valitsus (edaspidi *pooled*),

kooskõlas kahe- ja mitmepoolsete kokkulepetega, mis on juba sõlmitud poliitilistes ja julgeolekuküsimustes ning poliitilise, sõjalise ja majandusliku koostöö edendamiseks;

tõdedes poolte koostöö olulist osa rahu, rahvusvahelise julgeoleku ja vastastikuse usalduse tagamisel;

mõistes, et tulemuslik koostöö võib nõuda poolte salastatud teabe vahetamist;

soovides luua salastatud teabe vastastikust kaitset reguleerivaid eeskirju,

on kokku leppinud järgmises.

Artikkel 1. Eesmärk

Kokkuleppe eesmärk on tagada poolte koostöö käigus vahetatud või loodud salastatud teabe kaitse.

Artikkel 2. Mõisted

Kokkuleppes kasutatakse järgmisi mõisteid:
1) *salastatud teave*– mis tahes vormis teave, mida on vaja kaitsta salastatud teabe kaitse nõuete rikkumise eest ja mis on salastatud päritolupoole õigusaktide kohaselt;
2) *teadmisvajadus*– vajadus juurde pääseda salastatud teabele teenistuskohustuste tõttu ja teatava ülesande täitmiseks;
3) *riigi julgeoleku volitatud esindaja*– kokkuleppe rakendamise ja järelevalve eest vastutav riigiasutus;
4) *pädev asutus*– riigi julgeoleku volitatud esindaja või muu riigiasutus, mis vastutab riigi õigusaktide kohaselt järelevalve eest salastatud teabe valdkonnas ning kokkuleppe rakendamise eest;
5) *salastatud teabe kaitse nõuete rikkumine*– salastatud teabe mis tahes kujul avalikustamine, väärkasutamine, omavoliline muutmine, rikkumine, esitamine või hävitamine või muu tegevus või tegevusetus, mille tagajärjel kaob teabe salastatus, terviklikkus või kättesaadavus;
6) *salastatuse tase*– kategooria, mis poolte õigusaktide kohaselt määrab salastatud teabele juurdepääsu piirangu taseme ja poolte kohaldatavad miinimummeetmed selle kaitseks;
7) *juurdepääsuluba*– julgeolekueeskirjade alusel tehtav otsus, millega kinnitatakse isiku lojaalsust ja usaldusväärsust ning muid julgeolekuaspekte poolte õigusaktide kohaselt;
8) *töötlemisluba*– julgeolekueeskirjade alusel tehtav otsus, millega kinnitatakse, et juriidiline isik on võimeline kaitsma ja töötlema salastatud teavet poolte õigusaktide kohaselt;
9) *juurdepääsutunnistus*– dokument, millega kinnitatakse, et välisriigi juriidilisel või füüsilisel isikul on töötlemisluba või juurdepääsuluba ning tal on õigus juurde pääseda salastatud teabele ja kasutada seda Makedoonia Vabariigis;
10) *päritolupool*– pool, kes on loonud salastatud teabe;
11) *vastuvõttev pool*– pool, kellele edastatakse salastatud teavet;
12) *salastatud leping*– kahe või enama lepinglase kokkulepe, mis sisaldab salastatud teavet või võimaldab vastuvõtva poole lepinglasel juurde pääseda päritolupoole salastatud teabele;

13) *lepinglane*– füüsiline või juriidiline isik, kellel on õigus sõlmida lepinguid;
14) *kolmas isik*– riik, organisatsioon, juriidiline või füüsiline isik, kes ei ole selle kokkuleppe pool.

Artikkel 3. Salastatuse tasemed

Pooled lepivad kokku, et järgmised salastatuse tasemed on samaväärsed:

Makedoonia Vabariik	Eesti Vabariik	Ingliskeelne vaste
ДРЖАВНА ТАЈНА	TÄIESTI SALAJANE	TOP SECRET
СТРОГО ДОВЕРЛИВО	SALAJANE	SECRET
ДОВЕРЛИВО	KONFIDENTSIAALNE	CONFIDENTIAL
ИНТЕРНО	PIIRATUD	RESTRICTED

Artikkel 4. Riigi julgeoleku volitatud esindajad

1. Poolte riigi julgeoleku volitatud esindajad on:

– Makedoonia Vabariigis:
Salastatud teabe kaitse direktoraat, Vasko Karangeleski bb, Goce Delchev Barracks, 1000 Skopje, Makedoonia Vabariik;

– Eesti Vabariigis:
Kaitseministeeriumi julgeolekuosakond, Sakala 1, 15094 TALLINN, Eesti Vabariik.

2. Pooled teatavad teineteisele diplomaatiliste kanalite kaudu riigi julgeoleku volitatud esindaja muutmisest.

3. Riigi julgeoleku volitatud esindajad teavitavad teineteist kehtivatest riigi õigusaktidest, mis reguleerivad salastatud teabe kaitset, ning nende olulistest muudatustest.

4. Tihedama koostöö tagamiseks kokkuleppe rakendamisel võivad riigi julgeoleku volitatud esindajad pidada konsultatsioone.

5. Riigi julgeoleku volitatud esindajad võivad oma riigi õigusaktide kohaselt sõlmida kokkuleppe rakenduslepinguid.

6. Pool lubab taotluse korral teise poole julgeolekutöötajate külastusi, et koos võõrustava poole riigi julgeoleku volitatud esindajaga hinnata edastatud salastatud teabe kaitset.

Artikkel 5. Salastatud teabe kaitse meetmed

1. Pooled võtavad kooskõlas oma riigi õigusaktidega meetmeid, et kaitsta kokkuleppe alusel vahetatud või loodud salastatud teavet. Sellisele salastatud teabele tagatakse samasugune kaitse nagu oma teabele, mis on salastatud kokkuleppe artiklis 3 määratud samaväärsel tasemel.

2. Juurdepääs salastatud teabele antakse ainult füüsilisele või juriidilisele isikule, kellel on:
1) teadmisvajadus;
2) poolte õigusaktide kohaselt asjakohasel salastatuse tasemel antud juurdepääsuluba või töötlemisluba;
3) Makedoonia Vabariigis ka juurdepääsutunnistus.

3. Taotluse korral abistavad pädevad asutused teineteist julgeolekukontrolli tegemisel.

4. Eesti Vabariigis võib kooskõlas riigi õigusaktidega anda salastatud teabele juurdepääsu ilma juurdepääsuloata.

5. Päritolupoole riigi julgeoleku volitatud esindaja taotluse korral väljastab vastuvõtva poole riigi julgeoleku volitatud esindaja kirjaliku kinnituse selle kohta, et füüsilisel isikul on lõigete 2 ja 4 kohaselt õigus juurde pääseda salastatud teabele.

6. Vastuvõttev pool on kohustatud:
a) mitte edastama salastatud teavet kolmandale isikule ilma päritolupoole kirjaliku nõusolekuta;
b) kasutama salastatud teavet ainult sel eesmärgil, milleks see on antud.

Artikkel 6. Salastatud teabe edastamine

1. Salastatud teavet edastatakse kanalite kaudu, mis poolte riigi julgeoleku volitatud esindajad on kirjalikult kindlaks määranud.

2. Vastuvõttev pool kinnitab salastatud teabe kättesaamist kirjalikult.

3. Vajaduse korral võivad poolte julgeolekuasutused edastada teineteisele operatiivteavet ja/või luureandmeid otse.

Artikkel 7. Tõlkimine, paljundamine ja hävitamine

1. Tasemel СТРОГО ДОВЕРЛИВО / SALAJANE / SECRET või sellest kõrgemal tasemel salastatud teavet tõlgitakse ja paljundatakse ainult päritolupoole riigi julgeoleku volitatud esindaja kirjalikul loal.

2. Salastatud teavet tõlgivad füüsilised isikud, kellel on asjakohane juurdepääsuluba. Tõlkele tehakse salastusmärge ja sihtkeelne märkus, et tõlge sisaldab päritolupoole salastatud teavet.

3. Salastatud teavet paljundatakse koos salastusmärgetega või tehakse need igale eksemplarile. Paljundatud teavet kontrollitakse samamoodi nagu originaalteavet. Koopiate arv piirdub ametlikuks otstarbeks nõutavaga.

4. Kui lõikes 5 ei ole ette nähtud teisiti, hävitatakse salastatud teave poolte õigusaktide kohaselt viisil, mis ei võimalda seda osaliselt ega täielikult taastada.

5. Tasemel ДРЖАВНА ТАЈНА / TÄIESTI SALAJANE / TOP SECRET salastatud teavet ei hävitata. See tagastatakse päritolupoole pädevale asutusele.

6. Kriisiolukorras, kui kokkuleppe kohaselt loodud või edastatud salastatud teavet ei ole võimalik kaitsta ega tagastada, hävitatakse salastatud teave otsekohe. Vastuvõttev pool teatab päritolupoole riigi julgeoleku volitatud esindajale salastatud teabe hävitamisest võimalikult kiiresti.

Artikkel 8. Salastatud lepingud

1. Salastatud lepinguid sõlmitakse ja täidetakse kummagi poole õigusaktide kohaselt. Taotluse korral annab kummagi poole riigi julgeoleku volitatud esindaja teavet selle kohta, kas pakutud lepinglasel on asjakohasele salastatuse tasemele vastav juurdepääsuluba või töötlemisluba. Kui pakutud lepinglasel ei ole juurdepääsuluba ega töötlemisluba, võib poole riigi julgeoleku volitatud esindaja taotleda teise poole riigi julgeoleku volitatud esindajalt asjaomase lepinglase julgeolekukontrolli, et väljastada talle juurdepääsuluba või töötlemisluba.

2. Kui salastatud leping või alltöövõtuleping sisaldab tasemel ДОВЕРЛИВО/ KONFIDENTSIAALNE/ CONFIDENTIAL või sellest kõrgemal tasemel salastatud teavet või hõlmab sellele juurdepääsu, on lepingu lahutamatu osa julgeolekulisa. Selles lisas määrab päritolupoole lepinglane kindlaks vastuvõtvale poolele edastatava salastatud teabe ja selle salastatuse taseme.

3. Peale selle nähakse julgeolekulisas ette vähemalt:
a) lepinglase kohustus avaldada salastatud teavet ainult isikule, kes vastab artikli 5 lõikes 2 sätestatud nõuetele ning kes on tööle võetud salastatud lepingu täitmiseks või tegeleb selle täitmisega;
b) salastatud teabe edastamiseks kasutatavad kanalid;
c) muudatustest teatamise kord ja viisid, mida tuleb järgida, kui salastatud teabe salastatuse tase muutub või kui teavet ei ole enam vaja kaitsta;
d) kord, mille kohaselt ühe poole isikud võivad salastatud lepinguga seoses külastada või kontrollida teise poole lepinglaste ehitisi;
e) lepinglase pädeva asutuse kohustus teatada salastatud teabe kaitse nõuete rikkumisest, selle katsest või sellekohasest kahtlusest;
f) salastatud teabe kasutamine salastatud lepingu alusel ainult lepingu objektiga seotud eesmärgil;
g) range kinnipidamine salastatud teabe töötlemise korrast;
h) salastatud teabe andmine salastatud lepingu alusel kolmandale isikule ainult päritolupoole selgel nõusolekul.

4. Lepinglasega sõlmitud salastatud lepingus, mis sisaldab tasemel ИНТЕРНО/PIIRATUD/RESTRICTED salastatud teavet, on asjakohane säte, millega määratakse kindlaks sellise salastatud teabe kaitse miinimumnõuded.

Artikkel 9. Külastused

1. Poole isikute külastused teise poole lepinglase juurde, mis on seotud salastatud lepinguga ja millega kaasneb juurdepääs salastatud teabele, võivad toimuda ainult võõrustava poole pädevalt asutuselt saadud kirjaliku loa alusel.

2. Lõikes 1 nimetatud luba antakse üksnes isikule, kellel on lähetava poole õigusaktide kohaselt väljastatud asjakohane juurdepääsuluba.

3. Külastustaotlus sisaldab järgmisi andmeid:
a) külastuse eesmärk, kuupäev ja tegevuskava;
b) külastaja ees- ja perekonnanimi, sünniaeg ja -koht ning kodakondsus;
c) passi või isikutunnistuse number;
d) külastaja ametikoht ja selle üksuse nimi, keda ta esindab;
e) külastaja juurdepääsuloa tase;
f) külastatava juriidilise isiku nimi ja aadress;

g) külastatava isiku ees- ja perekonnanimi ning ametikoht;
h) muud andmed pädevate asutuste kokkuleppel.

4. Lõikes 3 nimetatud taotlus esitatakse piisavalt aegsasti.

Artikkel 10. Salastatud teabe kaitse nõuete rikkumine

1. Salastatud teabe kaitse nõuete rikkumise korral teavitab selle poole pädev asutus, kus nõudeid rikuti, teise poole pädevat asutust võimalikult kiiresti ning korraldab asjakohase uurimise. Teine pool teeb taotluse korral uurimise käigus koostööd.

2. Kui salastatud teabe kaitse nõudeid on rikutud kolmandas riigis, võtab lähetava poole pädev asutus lõikes 1 sätestatud meetmeid.

3. Igal juhul teavitatakse teist poolt uurimistulemustest ning saadetakse talle lõpparuanne kahjustuste põhjuste ja ulatuse kohta.

Artikkel 11. Kulud

Kumbki pool kannab kokkuleppest tulenevate kohustuste täitmisel tekkinud oma kulud.

Artikkel 12. Lõppsätted

1. Kokkulepe jõustub teise kuu esimesel päeval pärast seda, kui pooled on diplomaatiliste kanalite kaudu kätte saanud viimase kirjaliku teate selle kohta, et kokkuleppe jõustumiseks riigi õigusaktidega ettenähtud nõuded on täidetud.

2. Kokkulepe sõlmitakse määramata ajaks. Kumbki pool võib kokkuleppe lõpetada, teatades sellest teisele poolele kirjalikult diplomaatiliste kanalite kaudu. Sellisel juhul lõpeb kokkulepe lõpetamisteate kättesaamisest arvates kuue kuu pärast.

3. Lõpetamise korral kaitstakse kokkuleppe alusel edastatud või loodud salastatud teavet edasi kokkuleppe kohaselt.

4. Kokkulepet võib muuta poolte kirjalikul nõusolekul. Muudatused jõustuvad lõike 1 kohaselt.

5. Kokkuleppe tõlgendamise või rakendamisega seotud vaidlused lahendatakse poolte konsultatsioonide ja läbirääkimiste käigus kohtu poole pöördumata.

Koostatud 20. novembril 2008. aastal Skopjes kahes eksemplaris eesti, makedoonia ja inglise keeles; kõik tekstid on võrdselt autentsed.

Kokkuleppe tõlgenduserinevuste korral lähtutakse ingliskeelsest tekstist.

Eesti Vabariigi valitsuse nimel	**Makedoonia Vabariigi valitsuse nimel**
Urmas PAET	**Antonio MILOŠOSKI**

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

Done on 20 November 2008 at Skopje

The Government of the Republic of Estonia and the Government of the Republic of Macedonia (hereinafter referred to as “the Parties”),

In line with the bilateral and multilateral agreements already concluded on political and security-related issues and on enhancing the political, military and economic cooperation,

Recognising the important role of the mutual cooperation between the Parties for the stabilisation of peace, international security and mutual confidence,

Realising that good cooperation may require exchange of Classified Information between the Parties,

Desiring to create a set of rules regulating the mutual protection of Classified Information,

Have agreed as follows:

Article 1. Objective

The objective of this Agreement is to ensure the protection of Classified Information exchanged or generated in the course of co-operation between the Parties.

Article 2. Definitions

For the purpose of this Agreement:
1) “Classified Information” means any information, irrespective of the form, which requires protection against Security Compromise and has been classified in accordance with the national laws and regulations of the Originating Party;
2) “Need-to-know” means the necessity to have access to specific Classified Information in connection with official duties and for the performance of a specific task;
3) “National Security Authority” means the national authority responsible for the implementation and supervision of this Agreement;
4) “Competent Authority” means the National Security Authority or another national authority which, under the national laws and regulations, exercises supervision in the sphere of protection of classified information as well as conducts the implementation of this Agreement;
5) “Security Compromise” means any form of disclosure, misuse, unauthorised alteration, damage, submission, or destruction of Classified Information, as well as any other action or inaction, resulting in loss of its confidentiality, integrity or availability;
6) “Security Classification Level” means a category which, according to the national laws and regulations of the Parties, determines the level of restriction of access to Classified Information and the minimum security measures applied to it by the Parties;
7) “Personnel Security Clearance” means a positive determination stemming from a security procedure that shall ascertain loyalty and trustworthiness of an individual, as well as other security aspects, in accordance with national laws and regulations of the Parties;
8) “Facility Security Clearance” means a positive determination stemming from a security procedure that shall ascertain that a legal entity is able to protect and process Classified Information in accordance with national laws and regulations of the Parties;
9) “Access Permit” is a document confirming that the foreign legal entity or individual has a security clearance and is eligible to have access to and use Classified Information in the Republic of Macedonia;
10) “Originating Party” means the Party that has created the Classified Information;
11) “Receiving Party” means the Party to which Classified Information is transmitted;
12) “Classified Contract” means an agreement between two or more contractors, which contains Classified Information or involves access by the contractor of the Receiving Party to the Classified Information of the Originating Party;
13) “Contractor” means an individual or a legal entity possessing the legal capacity to conclude contracts;
14) “Third Party” means any state, organisation, legal entity and individual which is not a party to this Agreement.

Article 3. Security Classification Levels

The Parties agree that the following security classification levels are equivalent:

For the Republic of Macedonia	For the Republic of Estonia	Equivalent in English
ДРЖАВНА ТАЈНА	TÄIESTI SALAJANE	TOP SECRET
СТРОГО ДОВЕРЛИВО	SALAJANE	SECRET
ДОВЕРЛИВО	KONFIDENTSIAALNE	CONFIDENTIAL
ИНТЕРНО	PIIRATUD	RESTRICTED

Article 4. National Security Authorities

1. The National Security Authorities of the Parties are:

– For the Republic of Macedonia:
Directorate for Security of Classified Information, Vasko Karangeleski bb, Goce Delchev Barracks, 1000 Skopje, Republic of Macedonia;

– For the Republic of Estonia:
Security Department, Ministry of Defence, Sakala 1, 15094 TALLINN, Republic of Estonia.

2. The Parties shall inform each other through diplomatic channels of any changes of the National Security Authorities.

3. The National Security Authorities shall inform each other of the national laws and regulations in force regulating the protection of Classified Information as well as any substantial amendments to them.

4. In order to ensure closer cooperation in the implementation of this Agreement, the National Security Authorities may hold consultations.

5. The National Security Authorities may conclude executive documents, in accordance with their national laws and regulations, aimed at the implementation of this Agreement.

6. At the request of the other Party, each Party shall authorise visits of security personnel of the other Party to participate with the National Security Authority of the hosting Party in the assessment of the protection of the Classified Information transmitted.

Article 5. Measures for Protection of Classified Information

1. In compliance with their national laws and regulations, the Parties shall implement all appropriate measures for the protection of Classified Information, which is exchanged or generated under this Agreement. The same level of protection shall be ensured for such Classified Information as it has been provided for the national Classified Information with the corresponding security classification level, as defined in Article 3 of this Agreement.

2. Access to Classified Information shall be granted only to those individuals/legal entities, who:
1) have a need-to-know,
2) have been issued a Personnel Security Clearance / Facility Security Clearance of the appropriate security classification level in accordance with the national laws and regulations of the Parties, and,
3) in case of the Republic of Macedonia, also have an Access Permit.

3. On request, the Competent Authorities shall assist each other in carrying out security vetting procedures.

4. In case of the Republic of Estonia, access to Classified Information may be granted without a Personnel Security Clearance, subject to national laws and regulations.

5. On request of the National Security Authority of the Originating Party, the National Security Authority of the Receiving Party shall issue a written assurance that an individual has a right to access to Classified Information as set forth in paragraphs 2 and 4 of this Article.

6. The Receiving Party is obligated:
a) not to submit Classified Information to a Third Party without prior written consent of the Originating Party;
b) not to use the Classified Information for a purpose other than it has been provided for.

Article 6. Transmission of Classified Information

1. Classified Information shall be transmitted through channels determined in writing by the National Security Authorities of the Parties.

2. The Receiving Party shall confirm in writing the receipt of the Classified Information.

3. If necessary, the security services of the Parties may transmit operative and/or intelligence information directly to each other.

Article 7. Translation, Reproduction, Destruction

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

2. All translations of Classified Information shall be made by individuals possessing appropriate Personnel Security Clearances. Such translations shall bear an appropriate classification marking and a suitable annotation in the language of the translation, indicating that the translation contains Classified Information of the Originating Party.

3. When Classified Information is reproduced, the classification markings of the original shall also be reproduced or marked on each copy. Such reproduced information shall be placed under the same control as the original information. The number of the copies shall be limited to that required for official purposes.

4. Subject to paragraph 5 of this Article, Classified Information shall be destroyed pursuant to the national laws of the Parties in such a manner as to eliminate the partial or total reconstruction of the same.

5. Classified Information marked as ДРЖАВНА ТАЈНА / TÄIESTI SALAJANE / TOP SECRET shall not be destroyed. It shall be returned to the Competent Authority of the Originating Party.

6. In case of crisis situation, which makes it impossible to protect and return Classified Information exchanged or generated according to this 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 8. Classified Contracts

1. Classified Contracts shall be concluded and implemented in accordance with the national laws and regulations of each Party. Upon request the National Security Authority of each Party shall furnish information whether a proposed Contractor has been issued a national Personnel Security Clearance / Facility Security Clearance, corresponding to the required Security Classification Level. If the proposed Contractor does not hold a Personnel Security Clearance / Facility Security Clearance, the National Security Authority of each Party may send a request to the National Security Authority of the other Party for that Contractor to be security cleared for the issuance of a Personnel Security Clearance / Facility Security Clearance.

2. A security annex shall be an integral part of each Classified Contract or sub-contract containing or involving access to Classified Information classified as ДОВЕРЛИВО / KONFIDENTSIAALNE / CONFIDENTIAL and above. In this annex the Contractor of the Originating Party shall specify the Classified Information to be released to the Receiving Party and the security classification level that has been assigned to that information.

3. In addition the security annex shall regulate at least the following:
a) an obligation for the Contractor to disclose Classified Information only to an individual who meets the requirements set forth in paragraph 2 of Article 5 and who is employed or engaged in the performing of the Classified Contract;
b) the channels to be used for transfer of the Classified Information;
c) the procedures and mechanisms for communicating any changes in respect of the Classified Information either because of the changes in its security classification level or because its protection is no longer required;
d) the procedure for the approval of visits, access or inspections by individuals of one of the Parties to the facilities of the Contractor of the other Party that are related to the Classified Contract;
e) an obligation that the Contractor's Competent Authority is to be notified of any actual, attempted or suspected Security Compromise, related to the Classified Contract;
f) usage of Classified Information under the Classified Contract only for the purposes related to the subject of the contract;
g) strict adherence to the procedures for handling of Classified Information; and
h) release of Classified Information under the Classified Contract to any Third Party only with an explicit consent of the Originating Party.

4. Classified Contracts concluded with Contractors that include information classified as ИНТЕРНО / PIIRATUD / RESTRICTED, shall contain an appropriate clause identifying the minimum measures to be applied for the protection of such Classified Information.

Article 9. Visits

1. Visits by individuals of one of the Parties to the Contractor of the other Party that are related to the Classified Contract and involve access to Classified Information shall be allowed only if a prior written permission from the Competent Authority of the hosting Party has been obtained.

2. The permission referred to in paragraph 1 of this Article shall be granted exclusively to the person possessing an appropriate Personnel Security Clearance issued according to the national laws of the sending Party.

3. Request for a visit shall include:
a) purpose, date and program of the visit;
b) name and surname of the visitor, date and place of birth, citizenship;
c) passport number or identity card number;
d) position of the visitor and the name of the entity which he or she represents;
e) level of the Personnel Security Clearance held by the visitor;
f) name and address of the facility to be visited;
g) name, surname and position of the person to be visited;
h) other data, if agreed upon by the Competent Authorities.

4. The request referred to in paragraph 3 of this Article shall be transmitted sufficiently in advance.

Article 10. Security Compromise

1. In case of a Security Compromise, the Competent Authority of the Party, where the Security Compromise has occurred, shall inform the Competent Authority of the other Party as soon as possible and shall carry out the appropriate investigation. The other Party shall, if required, cooperate in the investigation.

2. In cases when the Security Compromise has occurred in a third state, the Competent Authority of the sending Party shall take the actions set forth in paragraph 1 of this Article.

3. In all cases the other Party shall be informed of the results of the investigation and shall receive the final report on the reasons and extent of the damages.

Article 11. Expenses

Each Party shall bear the expenses related to the implementation of its obligations under this Agreement.

Article 12. Final Provisions

1. This Agreement shall enter into force on the first day of the second month following the receipt of the last note by which the Parties inform each other through diplomatic channels that their internal legal requirements necessary for the entry into force of this Agreement have been fulfilled.

2. This Agreement is concluded for an unlimited period of time. It may be terminated by either Party upon giving written notice to the other Party through diplomatic channels. In such case, this Agreement shall terminate six months after the receipt of the termination notice.

3. In the event of termination thereof, Classified Information transmitted or generated on the basis of this Agreement shall continue to be protected pursuant to the provisions of this Agreement.

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

5. Any dispute regarding the interpretation or implementation of this Agreement shall be resolved by consultations and negotiations between the Parties without recourse to outside jurisdiction.

Done at Skopje in 20 November 2008, in two original copies, each in the Estonian, Macedonian and English languages, all texts being equally authentic.

In case of any divergence of interpretation of the provisions of this Agreement, the English text shall prevail.

For the Government of the Republic of Estonia	**For the Government of the Republic of Macedonia**
Urmas PAET	**Antonio MILOŠOSKI**