Väljaandja:	Vabariigi Valitsus
Akti liik:	välisleping
Teksti liik:	algtekst
Jõustumise kp:	22.11.2003
Avaldamismärge:	RT II 2003, 31, 159

Eesti Vabariigi valitsuse ja Tšehhi Vabariigi valitsuse vaheline salastatud teabe kaitse kokkulepe

(õ)1.02.10 14:45

"Eesti Vabariigi valitsuse ja Tšehhi Vabariigi valitsuse vahelise salastatud teabe kaitse kokkuleppe" eelnõu heakskiitmine ja volituste andmine

Välisministeeriumi teadaanne välislepingu jõustumise kohta

Välisministeeriumi teadaanne välislepingu lõppemise kohta

Eesti Vabariigi ja Tšehhi Vabariigi salastatud teabe vahetamise ja vastastikuse kaitse kokkulepe

Koostatud 29. juulil 2003. a Tallinnas, 22. novembril 2003. a

Eesti Vabariigi valitsus ja Tšehhi Vabariigi valitsus, edaspidi lepingupooled, soovides kaitsta salastatud teavet, mida lepingupooled vahetavad nii otsekanalite kui ka salastatud teabega tegelevate riigiasutuste ning eraõiguslike juriidiliste isikute ja avalik-õiguslike juriidiliste isikute kaudu, on kokku leppinud järgmises.

Artikkel 1. Kohaldamisala

1. Käesoleva kokkuleppe alusel sõlmivad lepingupooled ja nende riigiasutused ning eraõiguslikud juriidilised isikud ja avalik-õiguslikud juriidilised isikud lepinguid ja kokkuleppeid järgmistes valdkondades:
a) lepingupoolte koostöö riigikaitse-, julgeoleku- ja sõjandusküsimustes;
b) lepingupoolte riigiasutuste, era- ja avalik-õiguslike juriidiliste isikute ja eraisikute koostöö; seadmete ja oskusteabe müük; teabevahetus; ühisürituste korraldamine ja lepingute sõlmimine ning muu koostöö riigikaitse, julgeoleku ja sõjanduse valdkonnas.

2. Kokkulepe ei reguleeri lepingupoolte julgeoleku- ja luureteenistuste teabevahetust.

3. Kokkuleppe alusel ei või lepingupool teiselt lepingupoolelt saada salastatud teavet, mille on edastanud kolmas isik.

Artikkel 2. Mõisted

Käesolevas kokkuleppes on mõistetel järgmine tähendus:
salastatud teave
a) suuliselt või elektrooniliselt edastatud andmed või punktis b määratletud materjal;
b) *materjalina*käsitatakse punktis c määratletud dokumenti ning valmis või tootmisjärgus masinat, seadet, relva või relvasüsteemi;
c) mis tahes salvestisekandjal olevat teavet sisaldav dokument;
*leping*on lepinglaste kokkulepe, milles nähakse ette lepinguosaliste õigused ja kohustused;
*salastatud leping*on salastatud teavet sisaldav või selle teabega sisu poolest seotud kokkulepe;
*lepinglane*on füüsiline või juriidiline isik, kellel on õigus sõlmida lepinguid;
*salastatud teabe kaitse nõuete rikkumine*on riigi julgeolekut käsitlevate õigusaktidega vastuolus olev tegu või tegevusetus, mille tõttu võib salastatud teave ohtu sattuda;
*teabeleke*on olukord, kus salastatud teave või selle osa on muutunud või võib muutuda kättesaadavaks isikule, asutusele või ettevõttele või riigile, kellel ei ole teabele juurdepääsu luba või volitust;
*juurdepääsuluba*on julgeolekukontrolli tulemusel antud õigus, mis kooskõlas riigi õigusaktidega kinnitab füüsilise või juriidilise isiku usaldusväärsust ning teisi julgeolekuaspekte. Nimetatud luba võimaldab ilma julgeolekut ohustamata anda füüsilisele või juriidilisele isikule õiguse saada ja kasutada kindla salastatuse tasemega teavet;
*teadmisvajadus*on isiku põhjendatud tarvidus saada salastatud teavet ametikohustuste täitmiseks; lepingupool võimaldab teavet saada teabe edastaja seatud tingimustel.

Artikkel 3. Salastatud teabe kaitse

1. Lepingupool rakendab oma õigusaktide ja õiguspraktika kohaseid abinõusid, et kaitsta salastatud teavet, mida tema asutused või ettevõtted edastavad või saavad või loovad kokkuleppeid sõlmides ja muul viisil suheldes. Lepingupool kohaldab edastatud, saadud ja loodud teabele samu salastatuse taseme nõudeid, mis kehtivad tema salastatud teabe kohta artikli 5 järgi.

2. Isikule võimaldatakse saada salastatud teavet ja ta lubatakse rajatisele või muusse kohta, kus tehakse salastatud toiminguid või säilitatakse salastatud teavet, kui tal on asjakohane juurdepääsuluba ning kui tal on teadmisvajadus oma kohustuste või tööülesannete täitmiseks.

3. Lepingupool tagab kontrollkäike tehes ja muul viisil, et tema jurisdiktsiooni all olevad asutused ja ettevõtted, kes saavad, valdavad, töötlevad või kasutavad teise lepingupoole salastatud teavet, järgiksid riigi julgeolekut käsitlevaid õigusakte ja selle valdkonna õiguspraktikat.

4. Kui lepingupoole kodanik elab teise lepingupoole territooriumil või kui sellel territooriumil paikneb lepingupoole rajatis, osutab lepingupoole pädev asutus teise lepingupoole pädevale asutusele oma õigusaktide alusel abi, mis võimaldab sellel asutusel kontrollida füüsilise või juriidilise isiku usaldusväärsust ning kontrolli tulemuste põhjal väljastada juurdepääsuloa. Abi andmise kohta võivad pädevad asutused sõlmida eraldi kokkuleppe.

5. Lepingupool tunnustab füüsilise ja juriidilise isiku juurdepääsuluba, mis on väljastatud teise lepingupoole õigusaktide alusel. Juurdepääsulubade tasemed peavad olema kooskõlas artikliga 5.

6. Pädevad asutused edastavad teineteisele teabe, mis käsitleb vastastikku tunnustatud füüsilise ja juriidilise isiku juurdepääsulubade tühistamist või nende tasemete alandamist või nimetatud lubades tehtud teisi muudatusi.

Artikkel 4. Teabe avalikustamine

1. Lepingupool ei avalikusta käesoleva kokkuleppe alusel saadud salastatud teavet kolmandale riigile ega selle kodanikule ilma teabe edastanud poole kirjaliku nõusolekuta. Ühelt lepingupoolelt teisele edastatud salastatud teavet kasutatakse kindlaksmääratud eesmärgil.

2. Kui lepingupool või artiklis 1 nimetatud valdkonnas tegutsev lepingupoole asutus või ettevõte esitab salastatud lepingu, mis tuleb täita teise lepingupoole territooriumil, vastutab teine lepingupool salastatud teabe kaitse eest kooskõlas oma õigusaktidega.

3. Lepingupool võib teiselt poolelt saadud salastatud teabe edastada oma riigis tegutsevale lepinglasele, kui ta tagab, et:
a) lepinglase käsutuses olevad vahendid võimaldavad salastatud teavet nõuetekohaselt kaitsta;
b) enne salastatud teabele juurdepääsu võimaldamist on lepinglasele kohaldatud asjakohase taseme julgeolekukontrolli nõudeid;
c) salastatud teabele oma kohustuste tõttu juurdepääsu vajava isiku suhtes on läbi viidud asjakohane julgeolekukontroll;
d) isikule, kellel on juurdepääs salastatud teabele, on asjakohaselt selgitatud kohustust kaitsta salastatud teavet ja et isik on seda kirjalikult kinnitanud.

Artikkel 5. Salastatuse tasemed

1. Salastatud teave märgistatakse ühega järgmistest üksteisele vastavatest salastatuse tasemete märgetest:

EESTI KEELES	**TŠEHHI KEELES**	**INGLISE KEELES**
TÄIESTI SALAJANE	PŘÍSNĚ TAJNÉ	TOP SECRET
SALAJANE	TAJNÉ	SECRET
KONFIDENTSIAALNE	DŮVĚRNÉ	CONFIDENTIAL
PIIRATUD	VYHRAZENÉ	RESTRICTED

2. Salastatud teabe vastuvõtnud lepingupool või lepingupoole asutus või ettevõte ei või teabe salastatuse taset muuta ega teavet avalikustada ilma teabe edastanud lepingupoole kirjaliku nõusolekuta. Teabe edastanud lepingupool teatab teabe vastuvõtnud lepingupoolele teabe salastatuse taseme kõigist muudatustest.

3. Teabe vastuvõtnud lepingupool märgistab salastatud teabe võrdväärse salastatuse taseme märkega. Tõlge ja koopia tähistatakse sama salastatuse taseme märgisega kui originaal.

Artikkel 6. Pädevad asutused

1. Käesoleva kokkuleppe rakendamise ja järelevalve eest vastutavad pädevad asutused on:

Eesti Vabariigis:

Riigi julgeoleku volitatud esindaja, Riigisaladuse kaitse osakond, Kaitseministeerium, Eesti Vabariik, Sakala 1, 15094 Tallinn, EESTI;

Tšehhi Vabariigis:
Riiklik Julgeolekuamet, Pk 49, 150 06 Praha 56, TŠEHHI VABARIIK.

2. Lepingupoole pädev asutus tagab kokkuleppe alusel edastatava salastatud teabe kaitse kooskõlas oma õigusaktidega.

3. Salastatuse standardite võrdlemise huvides edastab lepingupoole pädev asutus teise poole pädevale asutusele teavet oma julgeolekukorralduse ja tegevuse kohta ning võimaldab teise lepingupoole pädevatel ametnikel külastada oma riiki.

Artikkel 7. Külastused

1. Lepingupool lubab teise lepingupoole esindajal külastada salastatud teabe tootmise, töötlemise või hoidmise või salastatud projektis ettenähtud ülesannete täitmise kohta oma pädeva julgeolekuasutuse kirjalikul nõusolekul. Luba antakse isikule, kellel on asjakohane juurdepääsuluba ja kellel on teadmisvajadus.

2. Saatjariigi pädev asutus teatab kooskõlas käesoleva kokkuleppe lisas ettenähtud menetluskorraga vastuvõtjariigi pädevale asutusele külastusest vähemalt kolm nädalat ette. Nimetatud lisa on kokkuleppe lahutamatu osa. Lisas käsitletud külastuse korda võib muuta lepingupoolte pädevate asutuste kirjalikul nõusolekul.

Artikkel 8. Lepingud

1. Kui lepingupoole pädev asutus kavatseb teise lepingupoole lepinglasega sõlmida salastatud lepingu või kui ta soovib salastatud projektis ettenähtud ülesande täitmiseks volitada oma riigi lepinglase sõlmima lepingu teise lepingupoole riigis, peab ta saama teise lepingupoole pädevalt asutuselt kirjaliku kinnituse, et lepinglasel on asjaomase tasemega juurdepääsuluba ning et lepinglasel on vahendid, mis võimaldavad selle salastatuse tasemega teavet töödelda ja säilitada.

2. Lepingupoolte asutuste ja eraettevõtete vahelises salastatud lepingus on soovitatav käsitleda salastatavat teavet ja käesoleva kokkuleppe alusel selle teabe kohta kehtestatavaid salastatuse tasemeid asjakohases jaotises.

3. Kui isikud soovivad sõlmida salastatud all-lepingu, teatab lepinglane nende nimed pädevale asutusele sellelt heakskiidu saamiseks. Kui all-leping on heaks kiidetud, täidab all-lepinglane samu julgeolekunõudeid kui lepinglane.

4. Lepingupoole pädev asutus saadab salastatud projekti koostamise kohta või kokkuleppe, lepingu või all-lepingu sõlmimise kohta teate selle lepingupoole pädevale asutusele, kus leping täidetakse.

5. Lepingupoole pädev asutus saadab salastatud lepingus julgeolekut käsitleva jaotise kaks koopiat selle lepingupoole pädevale asutusele, kus leping täidetakse.

Artikkel 9. Sidekanalid ja teabe edastamine

1. Üldjuhul vahetavad lepingupooled salastatud teavet diplomaatiliste kanalite kaudu.

2. Lepingupooled võivad salastatud teavet edastada ka oma asutuste esindajate kaudu. Vajaduse korral võib teavet edastama volitada projektis osaleva eraõigusliku juriidilise isiku esindaja.

3. Kui lepingupool kavatseb edastada salastatud teavet suures koguses, teatab ta sellest teisele lepingupoolele ette ja teabe edastamise peavad heaks kiitma mõlema lepingupoole pädevad asutused.

4. Salastatud teabe võib edastada muul viisil, kui lepingupoolte pädevad asutused on selle heaks kiitnud.

Artikkel 10. Julgeolekunõuete rikkumine

Kui lepingupool on rikkunud teiselt lepingupoolelt saadud salastatud teabe kaitse nõudeid ja seetõttu tekitanud teabelekke või muul viisil kahjustanud ühiseid huve, teatab lepingupoole pädev asutus sellest teise lepingupoole asutusele võimalikult kiiresti ning tagab, et juhtumit uuritakse. Lepingupoole taotluse korral teeb teine lepingupool temaga uurimiskoostööd. Lepingupool teavitab teise lepingupoole pädevat asutust uurimistulemustest ja edastab talle kokkuvõtte teabelekke põhjustest ja ulatusest.

Artikkel 11. Kulud

Kokkuleppes ettenähtud julgeolekuabinõude rakendamise kulud ja muud kokkuleppe täitmise kulud kannab see lepingupool, kellel on kulud tekkinud.

Artikkel 12. Vaidluste lahendamine

Lepingupooled lahendavad kokkuleppe tõlgendamise või kohaldamise vaidluse oma pädevate asutuste konsultatsioonide teel või kui kokkuleppele sel viisil ei jõuta, siis lepingupoolte volitatud esindajate läbirääkimiste teel; vaidlust ei anta lahendada lepingupoole kohtule, rahvusvahelisele kohtule ega kolmandale isikule.

Artikkel 13. Lõppsätted

1. Kokkuleppe sõlmitakse määramata ajaks. Lepingupooled kiidavad kokkuleppe heaks oma õigusaktide kohaselt ja kokkulepe jõustub selleks vajalike tingimuste täitmist kinnitava hilisema kirjaliku teate saamisest arvates kolmekümne päeva pärast.

2. Lepingupool võib kokkuleppe lõpetada kirjaliku teatega. Sellisel juhul lõpeb lepingu kehtivus teate saamisest arvates kuue kuu pärast.

3. Kokkulepet võib muuta lepingupoolte kirjalikul nõusolekul. Muudatus jõustub kooskõlas lõikega 1.

4. Kui kokkulepe lõpetatakse, tagastatakse selle alusel edastatud salastatud teave või ese teisele lepingupoolele võimalikult kiiresti. Muud salastatud teavet või eset kaitstakse kooskõlas kokkuleppega.

Koostatud Tallinnas 29. juulil 2003. a kahes eksemplaris eesti, tšehhi ja inglise keeles. Tõlgendamiserisuste korral võetakse aluseks ingliskeelne tekst.

Eesti Vabariigi valitsuse nimel	**Tšehhi Vabariigi valitsuse nimel**
Herman SIMM	**Vladislav LABUDEK**

Eesti Vabariigi valitsuse ja Tšehhi Vabariigi valitsuse vahelise salastatud teabe kaitse kokkuleppe lisa

KÜLASTUSNÕUDED

1. Lepingupool võimaldab teise lepingupoole külastajal pääseda salastatud toiminguid tegevasse või salastatud teavet säilitavasse või töötlevasse asutusse või ehitisse juhul, kui:
a) teise lepingupoole pädev asutus või muu pädev valitsusasutus on andnud sellele isikule asjakohase juurdepääsuloa ning isik on volitatud saama salastatud teavet kooskõlas oma riigi õigusaktidega;
b) isiku on volitanud külastusel osalema tema riigi pädev asutus või muu pädev valitsusasutus.

2. Külastuse kavandanud lepingupoole pädev asutus teavitab teise lepingupoole pädevat asutust külastusest käesolevas lisas sätestatud korras ja tagab, et nimetatud asutus saab külastustaotluse kätte vähemalt kolm nädalat enne visiiti.

3. Külastustaotluses esitatakse järgmised andmed:
a) külastaja ees- ja perekonnanimi, sünniaeg ja -koht, kodakondsus ning isiku tööandja nimi ja passi või muu isikut tõendava dokumendi number;
b) isiku juurdepääsuloa andmed;
c) külastuse objekt ja eesmärk;
d) külastuse alguse kuupäev ja külastuse kestus;
e) andmed kontaktisiku ja varasema suhtluse kohta ning muu teave, mille alusel on võimalik otsustada, kas külastus on põhjendatud.

4. Taotlus esitatakse:
a) Tšehhi saatkonna kaudu Tallinnas, kui Eesti Vabariiki soovib külastada Tšehhi kodanik;
b) Eesti saatkonna kaudu Prahas, kui Tšehhi Vabariiki soovib külastada Eesti kodanik;
c) lepingupoolte pädevate asutuste kokkuleppel võib kasutada ka muid võimalusi.

5. Külastusluba kehtib kuni kaksteist kuud.

SECURITY AGREEMENT ON PROTECTION OF CLASSIFIED INFORMATION BETWEEN THE GOVERNMENT OF THE REPUBLIC OF ESTONIA AND THE GOVERNMENT OF THE CZECH REPUBLIC
Done on 29 July 2003 in Tallinn

The Government of the Republic of Estonia and the Government of the Czech Republic, hereafter referred to as the Parties, in order to safeguard the classified information transmitted directly or through public entities or private companies that deal with classified information of the States of the Parties have agreed on the following:

Article 1. Applicability

1. This Agreement shall form the basis of any contract or agreement that may be concluded in the future between the Parties or public entities and/or private companies of the States of the Parties concerning the following subjects:
a) Co-operation between the States of the two Parties concerning national defence, security and military issues.
b) Co-operation, sales of equipment and know-how, exchange of information, joint ventures, contracts or any other relations between public entities, private companies and/or natural persons of the States of the Parties concerning national defence, security and military issues.

2. This Agreement does not cover direct co-operation between intelligence services of both Parties and exchange of intelligence information.

3. This Agreement shall not be invoked by either Party in order to obtain classified information that the other Party has received from a third party.

Article 2. Definitions

For the purpose of this Agreement:

*Classified information*means
a) any classified item, either an oral communication of classified contents or electromagnetic transmission of a classified message, or "material" as defined in b) below,
b) the term "material" includes "document" as defined in c) below, and any item of machinery, equipment, weapon or weapon-systems either manufactured or in the process of manufacture,
c) the term "document" means any form of recorded information regardless of the type of recording media.

*Contract*means an agreement between two or more contractors creating and defining enforceable rights and obligations between the contractors.

*Classified contract*means a contract which contains or involves classified information.

*Contractor*means a natural person or a legal entity possessing the legal capability to undertake contracts.

*Breach of security*of classified information means an act or an omission contrary to national legal security regulations, the result of which may endanger or compromise classified information.

*Security compromise*means that classified information is compromised because knowledge of it has passed, in the whole or in part, to persons or entities or states without appropriate security clearance or authority to have such access, or that it has been subjected to the risk of such passing.

*Security clearance*means a positive determination stemming from an investigative procedure that shall ascertain the loyalty and trustworthiness of a person or entity as well as other security aspects in accordance with the national legal regulations. Such determination enables that person or entity to be granted access and permission to handle classified information on a certain level without security risk.

"*Need-to-know*" means that access to classified information may only be granted to a person who has a verified need to know such information in connection with his official duties, within the framework of which the information was released to the receiving Party.

Article 3. Security Protection

1. In accordance with their national laws, legal regulations and practice, both Parties shall take appropriate measures to protect classified information, which is transmitted, received, produced or developed as a result of any agreement or relation between the Parties or entities of their States. The Parties shall afford to all transmitted, produced or developed classified information the same degree of security protection as is provided to their own classified information of the equivalent level of classification, as defined in Article 5 of this Agreement.

2. Access to classified information and to locations and facilities where classified activities are performed or where classified information is stored, shall be limited only to those persons who have been granted appropriate security clearance and who, due to their functions or employment, have a "need-to-know".

3. Each Party shall supervise the observance of national security laws, legal regulations and practice by the agencies, offices and facilities within their jurisdiction that possess, develop, produce and/or use classified information of the other Party, *inter alia*by means of review visits.

4. On request, the relevant Authorities of the States of the Parties, taking into account their national legal regulations, will assist each other during the vetting procedures of their citizens or facilities living or located in the territory of the other State, preceding the issue of the Personnel Security Clearance and the Facility Security Clearance. In this respect, specific arrangements may be agreed on between the Competent Security Authorities.

5. The Parties shall recognise the Personnel and Facility Security Clearance issued in accordance with national laws and legal regulations of the other State. The equivalence of the security clearances shall be in compliance with Article 5 of this Agreement.

6. The Competent Security Authorities shall inform each other about changes of mutually recognised Personnel and Facility Security Clearances, particularly in cases of their withdrawal or downgrading.

Article 4. Disclosure of Classified Information

1. The Parties shall not disclose classified information received under this Agreement to third parties or citizens of other states without the prior written consent of the originating Party. Classified information transmitted from one Party to the other Party shall be used for the specified purpose only.

2. In the event that either Party and/or agencies or entities from its State, concerned with the subjects set out in Article 1, award a classified contract to be performed within the territory of the State of the other Party, then the Party of the State in which the contracted performance is taking place, shall assume responsibility for protection of such classified information in accordance with its own national standards and legal regulations.

3. Prior to any release of classified information received from the other Party to contractors or prospective contractors from the State of the receiving Party, the receiving Party shall:
a) Ensure that such contractors or prospective contractors and their facilities have the capability to protect the classified information adequately;
b) Ensure that each contractor has undergone a security check of a corresponding level before having access to classified information;
c) Ensure that all persons who, because of their duties, require access to classified information have undergone a security check of a corresponding security level;
d) Ensure that all persons having access to classified information have been appropriately security briefed about their responsibilities to protect classified information and have confirmed this in writing.

Article 5. Security Classifications

1. Classified information shall be assigned one of the following equivalent security classification levels:

ESTONIAN	**CZECH**	**ENGLISH**
TÄIESTI SALAJANE	PŘÍSNĚ TAJNÉ	TOP SECRET
SALAJANE	TAJNÉ	SECRET
KONFIDENTSIAALNE	DŮVĚRNÉ	CONFIDENTIAL
PIIRATUD	VYHRAZENÉ	RESTRICTED

2. The receiving Party and/or entities from its State shall neither downgrade the classification nor declassify the received classified information without the prior written consent of the originating Party. The originating Party shall inform the receiving Party of any changes in security classification of the transmitted information.

3. The receiving Party shall mark the received classified information with its own equivalent security classification. Translations and reproductions shall be marked with the same security classification as the originals.

Article 6. Competent Security Authorities

1. The Competent Security Authorities responsible for the implementation and supervision of all aspects of this Agreement are:

In the Republic of Estonia:
National Security Authority, Department of Security, Ministry of Defence, Republic of Estonia, Sakala Str. 1, 15094 Tallinn, ESTONIA;

In the Czech Republic:
National Security Authority, P.O. Box 49, 150 06 Prague 56, CZECH REPUBLIC.

2. Both Competent Security Authorities, each within the jurisdiction of its own State, shall ensure appropriate protection of classified information transmitted according to this Agreement in compliance with their national legal regulations.

3. Each Competent Security Authority shall, on request, pass to the other Competent Security Authority information about its security organisation and procedures to make it possible to compare and maintain the same security standards and shall enable visits to its state by certified officials of the other Party.

Article 7. Visits

1. Visits to premises where classified information is developed, handled or stored or where classified projects are carried out, shall only be granted to visitors from the State of the other Party in case that prior written permission from the Competent Security Authority of the State of the host Party has been obtained. Such permission shall only be granted to persons who have been granted appropriate security clearance and have a "need-to-know".

2. The Competent Security Authority of the State of the sending Party shall notify the Competent Security Authority of the State of the host Party of expected visitors at least three weeks prior to the planned visit, in accordance with the procedures defined in the Annex to this Agreement. This Annex forms an integral part to this Agreement. Visit procedures as defined in the Annex can be changed on the basis of written consent of both Competent Security Authorities.

Article 8. Contracts

1. The Competent Security Authority of the State of one Party, wishing to place a classified contract with a contractor in the State of the other Party, or wishing to authorise one of its own contractors to place a classified contract in the State of the other Party within a classified project, shall obtain a prior written assurance from the Competent Security Authority of the State of the other Party that the proposed contractor holds security clearance of an appropriate level and has the suitable facilities to handle and store classified information of the same level.

2. Every classified contract between entities of the States of the Parties and/or private companies and/or natural persons should contain an appropriate security section identifying classified aspects of the contract and a list of security classifications allocated to them, based on the terms of this Agreement.

3. Names of the subcontractors interested in classified subcontracts shall be submitted in advance by the contractor to the Competent Security Authority for approval. If approved, the subcontractor must fulfil the same security obligations as the contractor.

4. Notification of any classified project, agreement, contract or subcontract shall be forwarded in advance to the Competent Security Authority of the State where the work is to be performed.

5. Two copies of the security section of any classified contract shall be forwarded to the Competent Security Authority of the State where the work is to be performed.

Article 9. Communications and Transmissions

1. Classified information shall normally be transmitted between the Parties through the diplomatic channels.

2. Transmission of classified information can also take place through representatives officially appointed by the authorities of the States of both Parties. Such authorisation may, when required, be given to representatives of private entities engaged in specific projects.

3. Delivery of large items or quantities of classified information arranged on a case by case basis shall be approved by both Competent Security Authorities.

4. Other means of transmission of classified information may be used if approved by both Competent Security Authorities.

Article 10. Breach of Security

In case of a breach of security concerning classified information originating or received from the other Party that results in a security compromise or if common interests are involved, the Competent Security Authority of the State where the compromise occurs shall inform the Competent Security Authority of the State of the other Party as soon as possible and take appropriate action to ensure that such an incident is properly investigated. The other Party shall, if required, co-operate in the investigation. In any case, the Competent Security Authority of the State of the other Party shall be informed of the results of the investigation and shall receive a final statement on the reasons and extent of the security violation.

Article 11. Expenses

Expenses incurred to a Party with respect to this Agreement, in particular concerning the implementation of security measures set herein, shall be covered by the self-same Party.

Article 12. Settlement of Disputes

Any dispute regarding the interpretation or application of this Agreement shall be resolved by consultations between the Competent Security Authorities of the States or, in the case that such a settlement is impossible to reach, between duly authorised representatives of the Parties, and shall not be referred to any national or international tribunal or third party for settlement.

Article 13. Final Provisions

1. This Agreement is concluded for an indefinite period. This Agreement is subject to approval in accordance with the national legal regulations of the States of both Parties and shall enter into force thirty days after the last written notification has been received indicating that the necessary legal conditions for this Agreement to enter into force have been fulfilled.

2. This Agreement may be terminated at any time by either Party with a written notification. In such a case the Agreement expires six months after receipt of this notification.

3. Amendments to the present Agreement may be made at any time with the consent of both Parties in written form. Such amendments shall enter into force in accordance with paragraph 1 of this Article.

4. In the event of termination, classified information and/or items transmitted under the terms of this Agreement shall be returned to the other Party as soon as possible. Remaining classified information and/or items shall be protected in accordance with the provisions of this Agreement.

Done in Tallinn on 29.07.2003 in two originals in the Estonian, Czech and English languages. In the case of different interpretations the English version of the Agreement shall prevail.

On behalf of Government of the Republic of Estonia
Herman SIMM

On behalf of Government of the Czech Republic
Vladislav LABUDEK

Annex
to the Security Agreement on Protection of Classified Information between the Government of the Republic of Estonia and the Government of the Czech Republic

VISIT REQUIREMENTS

1. Access to classified information and to establishments and facilities where classified activities are performed or where classified information is stored or handled, shall be allowed by one Party to visitors from the other Party only if they have been:
a) granted appropriate security clearance by the Competent Security Authority or other competent government authority of the sending Party and authorised to receive or to have access to classified information in accordance with the national legal regulations of their State;
b) authorised by the Competent Security Authority or other competent government authority of the respective State to perform the required visit or visits.

2. The Competent Security Authority of the sending Party shall notify the Competent Security Authority of the receiving Party of the planned visit in accordance with the provisions of this Annex, and shall ensure that the latter receives the visit request at least three weeks before the visit or visits take place.

3. The visit request shall include:
a) Visitor’s first and last name, place and date of birth, nationality, name of employer, passport number or number of another identity document of the visitor;
b) Visitor’s Personnel Security Clearance Certificate and its validity;
c) Object and purpose of the visit or visits;
d) Expected date and duration of the requested visit or visits;
e) Point of contact at the establishment/facility to be visited, previous contacts and any other information useful to determine the justification of the visit or visits.

4. The request shall be submitted:
a) Through the Estonian Embassy in Prague for visit requests of Estonian citizens to the Czech Republic;
b) Through the Czech Embassy in Tallinn for visit requests of Czech citizens to the Republic of Estonia;
c) Other procedures may be used if approved by both Competent Security Authorities.

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

Õiend
Metaandmetes parandatud akti andja: Vabariigi Valitsus.