No. 37392

Estonia
and
Lithuania

Agreement between the Government of the Republic of Estonia and the Government of the Republic of Lithuania on mutual protection of classified information. Tartu, 26 May 2000

Eutry into force: *15 November 2000 by notification, in accordance with article 10*

Authentic texts: *English, Estonian and Lithuanian*

Registration with the Secretariat of the United Nations: *Estonia, 4 April 2001*

Estonie
et
Lituanie

Accord entre le Gouvernement de la République d'Estonie et le Gouvernement de la République de Lituauie relatif à la protection mutuelle des iuformations classifiées. Tartu, 26 mai 2000

Entrée en vigueur : *15 novembre 2000 par notification, conformément à l'article 10*

Textes authentiques : *anglais, estonien et lituanien*

Enregistrement auprès du Secrétariat des Nations Unies : *Estonie, 4 avril 2001*

[ENGLISH TEXT — TEXTE ANGLAIS]

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

The Government of the Republic of Estonia and the Government of the Republic of Lithuania (hereinafter referred to as the "Parties"),

Aiming to tight political, military, economical, juridical, scientific and technological co-operation between the Parties;

Co-ordinating efforts towards NATO;

Realising that resulting co-operation may require exchange of classified information between the Parties;

Willing to ensure the protection of all classified information;

Have agreed as follows:

Article 1. General Provisions

1. The following terms are defined in the interests of clarity:

Classified information" means 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 which must for the interest of national security be exempted from disclosure and must enjoy protection against compromise.

Material" includes any item of machinery or equipment or weapons either manufactured or in the process of manufacture or document.

Document" means any recording medium containing classified information, including but not limited to any letter, note, minute, report, memorandum, signal/message, sketch, photograph, film, map, chart, notebook, stencil, carbon, typewriter ribbon, diskette etc or other form of recorded information (e.g. tape recording, magnetic recording, punched card, tape etc.).

Contractor" means an individual or legal entity possessing the legal capacity to undertake contracts.

"Classified contract" means a contract, which contains or involves classified information.

Competent Authority (CA)/ Designated Security Authority (DSA)" means the governmental authority responsible for security of information in each country.

Originating Party" means the Party initiating the classified information as represented by CA/DSA.

Recipient Party" means the Party to which the classified information is transmitted or transferred as represented by CA/DSA.

2. For the Republic of Lithuania, classified information is marked KONFIDENCIALIAI (CONFIDENTIAL), SLAPTAI (SECRET), VISISKAI SLAPTAI (TOP SECRET). For the Republic of Estonia, it is marked KONFIDENSIAALNE (CONFIDENTIAL), SALAJANE (SECRET), TAIESTI SALAJANE (TOP SECRET).

3. The Republic of Estonia will protect Lithuanian classified information KONFIDENCIALIAI as Estonian KONFIDENSIAALNE, Lithuanian classified information SLAPTAI as Estonian SALAJANE and Lithuanian classified information VISISKAI SLAPTAI as Estonian TAIESTI SALAJANE.

4. The Republic of Lithuania will protect Estonian classified information KONFIDENSIAALNE as Lithuanian KONFIDENCIALIAI, Estonian classified information SALAJANE as Lithuanian SLAPTAI and Estonian classified information TAIESTI SALAJANE as Lithuanian VISISKAI SLAPTAI.

5. The level of classification will be changed or revoked by the Recipient Party on request of the Originating Party. Change or revocation of classification level is to be notified to the Recipient Party within six weeks from the date of change or revocation of classification.

6. All classified information transmitted or transferred before this Agreement enters into force is to be protected in compliance with its provisions.

Article 2. National Responsibilities

1. The Parties shall undertake within the national law all necessary steps to ensure the protection of classified information which is to be transferred pursuant to this Agreement or to which a contractor gains access under a contract involving classified information. On occasion the Originating Party may ask the Recipient Party to afford protection at a higher level than the classification indicated.

2. Only authorised individuals can be granted access to classified information. The authorisation shall be granted only to individuals who have been appropriately security cleared and who have been authorised by the authority of his parent nation to have access to classified information. No individual is entitled solely by virtue of rank or appointment or security clearance to have access to classified information. Access to it shall be granted only to those individuals who require to be acquainted with the information in order to perform their duties.

3. The Parties will not release the received classified information to authorities or entities of a third party without prior written approval of DSA , which has assigned a security classification. Such classified information can be used only for the specified purpose.

Article 3. Classified contracts

1. Should the Party consider concluding a classified contract with a contractor residing in the territory of the country of the other Party or with contractor of the other Party residing in the territory of the country of the host Party, an assurance from CA shall be obtained in advance that the proposed contractor has a security clearance corresponding to the required classification level and has implemented appropriate security arrangements to ensure the

protection of the classified information. This assurance also involves the obligation to ensure that the security arrangements of the security cleared contractor

correspond to national legislation on protection of classified information and that these arrangements are supervised by CA.

2. DSA of the contractor is responsible for ensuring that each piece of classified information, which has been either released to the contractor of the other Party or generated in connection with a contract, has been assigned a security classification. By request of DSA of the contractor, DSA of the other Party shall provide a security requirements list. DSA of the other Party shall also provide DSA of the contractor with a notification stating that the contractor has undertaken to observe national legislation on the protection of classified information. DSA of the other Party shall submit an appropriate notification of the contractor's obligation to protect classified information to DSA of the contractor.

3. DSA of the contractor shall confirm in writing the receipt of the requested security requirements list and forward list to the contractor.

4. At all events, DSA of the contractor shall ensure that the contractor will handle the parts of the contract, which require classification, in the same manner as classified information of the country of the contractor in compliance with the classification level fixed in the security requirements list.

5. Should DSA approve a classified subcontract the paragraphs 2 and 4 of this Article shall apply accordingly.

6. The Parties will assure that a classified contract is concluded or, eventually, work on classified parts begins only after the contractor has implemented security measures.

Article 4. Translation, Reproduction and Destruction

1. Documents containing "T0P SECRET " information shall be allowed for translation and copying only on the written permission of DSA of the Originating Party.

2. All translations and reproductions of classified information shall be made by individuals with security clearance issued pursuant to Article 2 of this Agreement. Such translations and reproductions should bear appropriate security classification. The number of copies of such translations and reproductions shall be limited to that required for official purposes.

3. Classified documents shall be destroyed by burning, shredding or pulping so as to prevent reconstruction of classified information contained therein.

4. Classified material shall be destroyed beyond recognition or modified so as to prevent reconstruction of classified information in whole or in part.

5. The "TOP SECRET" documents and material usually shall not be destroyed -- they shall be returned to the sender after they are recognised as no longer necessary or upon the expiry of their validity.

Article 5. Transmission and transfer

1. Classified information is to be transferred from one Party to the other usually by means of diplomatic or military courier service or through military attachés. The Receiving Party shall confirm the receipt of classified information and forward the information to the recipient in accordance with national legislation concerning the protection of classified information.

2. DSAs are entitled to approve -- in connection with a specific case, generally or with some restrictions set up -- transfer of classified information by other means than diplomatic or military courier channels, provided the use of these courier services would result in inadequate complications pertaining to transfer or completion of the contract.

3. In cases described in paragraph 2 of this Article the following requirements are to be met:

The forwarder is to be authorised access to classified information of an appropriate classification level;

The Originating Party shall retain a list of classified information being transferred and a copy of this list shall be provided to the recipient who is to forward it to DSA;

The classified information shall be wrapped and sealed in compliance with regulations concerning internal transfer;

The hand over of classified information is to be confirmed in writing.

4. If transfer of a large quantity of classified information is required, DSAs shall mutually agree on and approve the means of transportation, the route and security escort for each such case.

5. Electronic transmission of classified information shall be carried out entirely in encrypted form (using cryptographic means and devices).

Article 6. Visits

1. If authorisation for visits should be given to representatives of one Party to visit facilities and establishments of the other Party, where access to classified information is required, it shall be limited to official purposes. Authorisations to visit the facilities and establishments shall be granted only by the respective CA/DSA. Prior to such visits an approval of CA/DSA of the host country will be required.

2. A visitor's request will include the following information:

Visitor's name and surname, date and place of birth and passport number;

Official status of the visitor together with the name of the establishment, company or organisation which the visitor represents or to which the visitor belongs;

Certificate indicating the level of security clearance of a visitor;

Purpose of the visit and the assumed date of arrival and departure;

Name and address (if applicable) of the establishment, company or organisation to be visited.

Article 7. Breach and Compromise

1. If a violation of regulations on the protection of classified information, which could result in loss or disclosure or possible loss or disclosure of such information released by the other Party, cannot be ruled out, is presumed, occurs or if classified information is compromised by any other way, the other Party shall be informed immediately.

2. Violations of regulations dealing with the protection of classified information shall be detected and prosecution conducted in compliance with legal regulations of the Party concerned. Results are to be reported to the other Party as soon as possible.

Article 8. Expenses

Costs of the implementation of this Agreement by one Party are not to be covered by the other Party.

Article 9. Competent Authorities

1. For the purpose of this Agreement, competent authorities of the Parties are:

In the Republic of Estonia:

Bureau of National Security Co-ordinator

Lossi Plats 1 A

EE-15161 TALLINN

Republic of Estonia;

In the Republic of Lithuania:

Commission for Co-ordinating of Protection of Secrets

Vytenio g. 1, 2600 Vilnius

Republic of Lithuania.

Article 10. Final provisions

1. This Agreement shall enter into force on the day of exchange of notes on complying with national legal requirements necessary for this Agreement to come into effect.

2. This Agreement is concluded for an unlimited period of time.

3. Any dispute regarding the interpretation or implementation of this Agreement shall be resolved by negotiations between the Parties.

4. Amendments to this Agreement maybe made by mutual consent of the Parties.

5. Each of the Parties is entitled to terminate the Agreement in writing, observing the six-month notice period. Despite of the termination of the Agreement, all classified information communicated pursuant to this Agreement or generated by the contractor shall continue to be handled in accordance with the provisions set forth in this Agreement as long as it is required by its classification allocation.

6. CAs and/or DSAs may conclude supplemental agreements or arrangements under this Agreement.

Done at Tartu on May 26, 2000 in two originals in Estonian, Lithuanian and English language. In case of disputes the English text shall prevail.

For the Government of the Republic of Estonia:

[TOOMAS HENRIK ILVES]

For the Government of the Republic of Lithuania:

[ALGIRDAS SAUDARGAS]

[ESTONIAN TEXT — TEXTE ESTONIEN]

EESTI VABARIIGI VALITSUSE

JA

LEEDU VABARIIGI VALITSUSE

SALASTATUD TEABE VASTASTIKUSE KAITSE

KOKKULEPE

Eesti Vabariigi valitsus ja Leedu Vabariigi valitsus (edaspidi "lepingupooled"),

eesmärgiga tugevdada lepingupoolte vahel poliitilist, sõjalist, majandus-, õigus-, teadus- ja tehnoloogiakoostööd;

ühitades NATOga liitumiseks tehtavaid pingutusi;

mõistes, et tulemuslikuks koostööks on vaja lepingupooltel vahetada salastatud teavet;

soovides kaitsta salastatud teavet,

leppisid kokku järgmises.

ARTIKKEL 1
ÜLDSÄTTED

1. Selguse huvides on defineeritud järgmised mõisted.

- **"Salastatud teave"** tähendab salastatud teavet, mis on edastatud kas suuliselt või nähtavana või elektrilisel või elektroonilisel teel, või materjali, mille avalikustamist peab riikliku julgeoleku huvides vältima ja mida peab lekke eest kaitsma.
- **"Materjal"** tähendab masina, varustuse või relva valmis või tootmisjärgus osist või dokumenti.
- **"Dokument"** tähendab jäädvustatud salastatud teavet, mis võib esineda kirja, noodi, protokolli, ettekande, memorandumi, leppemärgi või teate, toodetava eseme visandi, foto, filmi, kaardi, diagrammi, märkmiku, toodetava eseme šablooni, kopeerpaberi, kirjutusmasina lindi, disketi või muul kujul (nt lindistus, magnetsalvestis, perfokaart, lint jms).
- **"Lepingupartner"** tähendab füüsilist või juriidilist isikut, kellel on õigus sõlmida lepingut.
- **"Salastatud leping"** tähendab lepingut, mis sisaldab salastatud teavet või mille sisu on sellega seotud.
- **"Pädev asutus või määratud julgeolekuasutus** (viimasena nimetatu edaspidi **"julgeolekuasutus"**) tähendab valitsusasutust, kes asjaomases riigis vastutab salastatud teabe kaitse eest.
- **"Teavet edastav lepingupool"** tähendab pädeva asutuse või julgeolekuasutuse kaudu esindatavat lepingupoolt, kes salastatud teavet edastab.
- **"Teavet vastuvõttev lepingupool"** tähendab pädeva asutuse või julgeolekuasutuse kaudu esindatavat lepingupoolt, kellele salastatud teave edastatakse.

2. Leedu Vabariigi salastatud teabe kandjale tehakse märge "KONFIDENCIALIAI" (KONFIDENTSIAALNE), "SLAPTAI" (SALAJANE) või "VISIŠKAI SLAPTAI" (TÄIESTI SALAJANE). Eesti Vabariigi salastatud teabe kandjale tehakse märge "KONFIDENTSIAALNE" (CONFIDENTIAL), "SALAJANE" (SECRET) või "TÄIESTI SALAJANE" (TOP SECRET).

3. Eesti Vabariik kaitseb Leedu salastatud teavet märkega "KONFIDENCIALIAI" samuti nagu Eesti salastatud teavet märkega "KONFIDENTSIAALNE", Leedu salastatud teavet märkega "SLAPTAI" samuti nagu Eesti salastatud teavet märkega "SALAJANE" ning Leedu salastatud teavet märkega "VISIŠKAI SLAPTAI" samuti nagu Eesti salastatud teavet märkega "TÄIESTI SALAJANE".

4. Leedu Vabariik kaitseb Eesti salastatud teavet märkega "KONFIDENSIAALNE" samuti nagu Leedu salastatud teavet märkega "KONFIDENCIALIAI", Eesti salastatud teavet märkega "SALAJANE" samuti nagu Leedu salastatud teavet märkega "SLAPTAI" ning Eesti salastatud teavet märkega "TÄIESTI SALAJANE" samuti nagu Leedu salastatud teavet märkega "VISIŠKAI SLAPTAI".

5. Teabe vastuvõtnud lepingupool muudab salastatuse taset või tühistab selle teabe edastanud lepingupoole nõudmisel. Salastatuse taseme muutmisest või tühistamisest peab teabe vastuvõtnud lepingupoolele teatama salastatuse taseme muutmise või tühistamise kuupäevast arvates kuue nädala jooksul.

6. Enne julgeolekukokkuleppe jõustumist edastatud salastatud teavet kaitstakse kokkuleppe nõuete kohaselt.

ARTIKKEL 2
RIIKLIK VASTUTUS

1. Lepingupool täiendab oma siseriiklikku õigust nii, et see kaitseks kokkuleppe alusel vahetatud salastatud teavet ning teavet, millele lepingupartner pääseb juurde salastatud teavet sisaldava lepingu alusel. Vajaduse korral võib teavet edastanud lepingupool paluda teabe vastuvõtnud lepingupoolt, et ta kaitseks teabe edastanud lepingupoole salastatud teavet rangemalt, kui seda eeldab teabekandjale tehtud salastatuse taseme märge.

2. Juurdepääs salastatud teabele võimaldatakse ainult riigisaladusele juurdepääsuõigust omavale isikule. Juurdepääsuõigus antakse isikule, kes on läbinud asjakohase julgeolekukontrolli ja keda on tema asukohamaa volitanud salastatud teabele juurde pääsema. Kellelegi ei tohi võimaldada juurdepääsu salastatud teabele ainult tema auastme või ametikoha või juurdepääsuloa alusel. Juurdepääs salastatud teabele võimaldatakse ainult sellele isikule, kes vajab teavet oma tööülesannete täitmiseks.

3. Lepingupool ei tohi saadud salastatud teavet edastada kolmanda poole ametivõimudele ega asutustele teabe salastanud julgeolekuasutuse nõusolekuta. Kolmas pool võib salastatud teavet kasutada ainult kindlaksmääratud eesmärgil.

ARTIKKEL 3
SALASTATUD LEPINGUD

1. Lepingupool, kes soovib sõlmida salastatud lepingu teise lepingupoole riigi territooriumil asuva lepingupartneriga või tema oma riigi territooriumil asuva teise lepingupoole lepingupartneriga, peab saama pädeva asutuse kinnituse selle kohta, et soovitaval lepingupartneril on asjakohane julgeolekuluba ja ta on rakendanud salastatud teabe kaitseks vajalikud abinõud. Selline kinnitus tähendab ka seda, et julgeolekukontrolli läbinud lepingupartner on võtnud endale kohustuse rakendada abinõud, mis vastavad siseriiklikele salastatud teabe kaitset reguleerivatele õigusaktidele ja on pädeva asutuse järelevalve all.

2. Lepingupartneri julgeolekuasutus vastutab selle eest, et salastatud teabe iga selline osa, mille teine lepingupool on lepingupartnerile andnud või mis on loodud seoses salastatud lepinguga, kannaks kindlaksmääratud salastatuse taseme märget. Lepingupartneri julgeolekuasutuse taotluse korral esitab teise lepingupoole julgeolekuasutus julgeolekunõuete loetelu. Samuti edastab teise lepingupoole julgeolekuasutus lepingupartneri julgeolekuasutusele teatise selle kohta, et lepingupartner on kohustatud järgima siseriiklikke salastatud teabe kaitset reguleerivaid õigusakte. Teise lepingupoole julgeolekuasutus esitab lepingupartneri julgeolekuasutusele asjakohase teatise selle kohta, et lepingupartner on kohustatud salastatud teavet kaitsma.

3. Lepingupartneri julgeolekuasutus kinnitab taotletud julgeolekunõuete loetelu kättesaamist kirjalikult ja edastab loetelu lepingupartnerile.

4. Lepingupartneri julgeolekuasutus tagab, et lepingupartner kaitseb lepingu salastatust eeldavaid osi samaväärselt selle riigi, mille kodanik või juriidiline isik lepingupartner on, salastatud teabega ning vastavalt julgeolekunõuete loetelus kindlaksmääratud salastatuse tasemele.

5. Julgeolekuasutuse kinnitatud salajase all-lepingu suhtes kohaldatakse käesoleva artikli paragrahve 2 ja 4.

6. Lepingupool tagab, et salastatud leping sõlmitakse ja lepingu salastatud osi hakatakse rakendama pärast seda, kui lepingupartner on võtnud kasutusele julgeolekumeetmed.

ARTIKKEL 4
TÕLKIMINE, PALJUNDAMINE JA HÄVITAMINE

1. Dokumenti, mis sisaldab teavet märkega "TÄIESTI SALAJANE", tohib tõlkida ja paljundada ainult teabe edastanud lepingupoole julgeolekuasutuse kirjalikul loal.
2. Salastatud teavet tohib tõlkida ja paljundada isik, kellel on selle kokkuleppe artiklis 2 kirjeldatud juurdepääsuluba. Sellisele tõlkele või koopiale tehakse märge salastatuse taseme kohta. Koopia või tõlke eksemplaride arv määratakse kindlaks, lähtudes tööülesannete täitmiseks vajalikust kogusest.

3. Salastatud dokumente hävitatakse põletamise, purustamise või paberimassiks muutmise teel sel viisil, et selles sisalduvat salastatud teavet ei oleks võimalik taastada.

4. Salastatud materjale hävitatakse tundmatuseni või muudetakse sel viisil, et salastatud teavet ei oleks võimalik täielikult või osaliselt taastada.

5. Dokumenti või materjali märkega "TÄIESTI SALAJANE" tavaliselt ei hävitata. Kui selline dokument või materjal ei ole enam vajalik või kui selle salastamistähtaeg on möödunud, tagastatakse see saatjale

ARTIKKEL 5
EDASTAMINE

1. Salastatud teavet edastatakse ühelt lepingupoolelt teisele tavaliselt diplomaatilise või sõjalise kullerteenistuse või sõjaväeatašee kaudu. Teavet vastuvõttev lepingupool peab kinnitama salastatud teabe kättesaamist ja saatma teabe selle adressaadile siseriiklike salastatud teabe kaitset reguleerivate õigusaktide kohaselt.

2. Eeldusel, et diplomaatilise või sõjalise kullerteenistuse kasutamine võib põhjustada teabe edastamisel või lepingu täitmisel asjakohatuid takistusi, on julgeolekuasutusel erijuhul õigus kas piiranguid seades või tavalises korras kokku leppida salastatud teabe edastamises nimetatud kullerteenuse kanaleid kasutamata.
3. Käesoleva artikli paragrahvis 2 nimetatud juhul tuleb täita järgmisi nõudeid:
   - teabe kättetoimetajal peab olema vähemalt asjakohase salastatuse tasemega teabele juurdepääsu õigus;
   - salastatud teabe edastanud lepingupool säilitab edastatud teabe loetelu ning esitab selle koopia teabe vastuvõtjale, kes toimetab selle edasi teabe vastuvõtnud lepingupoole julgeolekuasutusele;
   - salastatud teave pakitakse ja pitseeritakse nimetatud teabe riigisisest edastamist reguleerivate õigusaktide kohaselt;
   - salastatud teabe üleandmist kinnitatakse kirjalikult;

- suure hulga salastatud teabe edastamise korral lepivad julgeolekuasutused kasutatava sõiduvahendi, marsruudi ja julgeoleku saatemeeskonna suhtes iga juhtumi puhul eraldi kokku;
- elektroonilisel teel edastatakse salastatud teavet täielikult krüpteeritud vormis, kasutades krüpteerimisvahendeid ja -varustust.

ARTIKKEL 6
VISIIT

1. Teise lepingupoole esindajal lubatakse külastada lepingupoole ehitisi ja asutusi, kus on vaja salastatud teabele juurdepääsuõigust, ainult ametiülesannete täitmiseks. Ehitise või asutuse visiidiloa annab ainult vastuvõtva riigi pädev asutus või julgeolekuasutus. Sellise visiidi tegemiseks on vaja saada vastuvõtva riigi pädeva asutuse või julgeolekuasutuse nõusolek.
2. Visiiditaotlus peab sisaldama:
   - külastaja perekonna- ja eesnime, sünnikohta ja -kuupäeva ning passinumbrit;
   - külastaja ametikohta ning selle asutuse, ettevõtte või organisatsiooni nime, mida külastaja esindab või kuhu ta kuulub;
   - kinnitust külastaja juurdepääsuloa taseme kohta;
   - visiidi eesmärgi selgitust ning oletatavat saabumis- ja lahkumisaega;
   - külastatava asutuse, ettevõtte või organisatsiooni nime ning aadressi selle olemasolu korral.

ARTIKKEL 7
JULGEOLEKUNÕUETE RIKKUMINE JA TEABELEKE

1. Kui ei ole välistatud salastatud teabe kaitse nõuete rikkumine, mille tagajärjel võib teiselt lepingupoolelt saadud teave kaduda või tulla avalikuks või tekib selleks võimalus; kui nimetatud nõudeid on juba rikutud või kui salastatud teave on lekkinud mõnel muul viisil, siis teavitatakse teist lepingupoolt juhtunust viivitamatult.

2. Salastatud teabe kaitse nõuete rikkumise asjaolud selgitatakse välja ning süüdlased võetakse asjaomase lepingupoole õigusaktide kohaselt vastutusele.
   Uurimistulemustest teavitatakse teist lepingupoolt esimesel võimalusel.

ARTIKKEL 8
KULUTUSED

Lepingupool ei kata neid kulusid, mida teine lepingupool on teinud selle kokkuleppe rakendamiseks.

ARTIKKEL 9
PÄDEVAD ASUTUSED

1. Selles kokkuleppes on lepingupoole pädevad asutused:

   Eesti Vabariigis:
   Koordinatsioonidirektori büroo
   Lossi plats 1 A
   EE-15161 TALLINN
   Eesti Vabariik

   Leedu Vabariigis:
   Saladuste kaitse koordineerimise komisjon
   Vytenio g. 1, 2600 Vilnius
   Leedu Vabariik.

ARTIKKEL 10
LÕPPSÄTTED

1. Kokkulepe jõustub päeval, mil vahetatakse selle kokkuleppe jõustumiseks vajalike siseriiklike õigusprotseduuride täitmist kinnitavad noodid.
2. Kokkulepe jääb kehtima piiramata ajaks.
3. Kokkuleppe rakendamise või tõlgendamisega seotud erimeelsused lahendatakse lepingupooltevaheliste läbirääkimiste teel.
4. Kokkulepet võib muuta lepingupoolte vastastikusel kokkuleppel.
5. Lepingupool võib kokkuleppe lõpetada, teatades sellest kirjalikult kuus kuud ette. Olenemata kokkuleppe lõppemisest kaitstakse kokkuleppe kehtimise ajal edastatud või loodud salastatud teavet kokkuleppe nõuete kohaselt selle teabe salastamistähtaja lõppemiseni.
6. Pädevad asutused või julgeolekuasutused võivad selle kokkuleppe alusel sõlmida lisakokkuleppeid.

Koostatud 26. mail 2000 Tartus kahes võrdväärses eksemplaris eesti-, leedu- ja inglise keeles. Erimeelsuste korral võetakse aluseks ingliskeelne tekst.

Eesti Vabariigi valitsuse nimel

Leedu Vabariigi valitsuse nimel

[LITHUANIAN TEXT — TEXTE LITUANIEN]

ESTIJOS RESPUBLIKOS VYRIAUSYBĖS

IR

LIETUVOS RESPUBLIKOS VYRIAUSYBĖS

SUTARTIS

DĖL ABIPUSĖS ĮSLAPTINTOS INFORMACIJOS APSAUGOS

Estijos Respublikos Vyriausybė ir Lietuvos Respublikos Vyriausybė (toliau vadinamos Šalimis),

siekdamos stiprinti Šalių politinį, karinį, ekonominį, juridinį, mokslinį ir technologinį bendradarbiavimą;

koordinuodamos savo pastangas siekiant narystės NATO;

suprasdamos, kad toks bendradarbiavimas gali pareikalauti abipusio keitimosi įslaptinta informacija;

norėdamos užtikrinti įslaptintos informacijos apsaugą,

s u s i t a r ė:

1 straipsnis

Bendrosios nuostatos

1. Dėl aiškumo pateikiami terminų apibrėžimai:

Įslaptinta informacija - visa įslaptinta medžiaga, nesvarbu, ar ji žodinė, vizuali, perduodama elektrinėmis ar elektroninėmis informacijos perdavimo priemonėmis, arba materiali medžiaga, kuri dėl nacionalinių saugumo interesų negali būti atskleista ir turi būti patikimai saugoma.

Terminas „**Medžiaga**" apima bet kokią pagamintą ar gamybos procese esančią techniką, įrangą ar ginklus bei dokumentus.

Dokumentas - bet kokiomis priemonėmis užfiksuota informacija, turinti slaptos informacijos, įskaitant, tačiau nesiribojant vien tik laiškais, užrašais, protokolais, ataskaitomis, memorandumais, signaliniais pranešimais, eskizais, nuotraukomis, fotojuostomis, žemėlapiais, schemomis, užrašų knygelėmis, trafaretais, kalkėmis, rašomųjų mašinėlių juostelėmis, kompiuterių laikmenomis ir pan. ar kita forma įrašyta informacija (pvz., magnetofoniniai, magnetiniai įrašai, perforacinės kortelės, juostos ir t.t.)

Sutarties dalyvis - fizinis ar juridinis asmuo, turintis teisę sudaryti sutartis.

Įslaptinta sutartis - sutartis, kurioje yra įslaptintos informacijos, arba sutartis, susijusi su tokia informacija.

Kompetentinga institucija (KI)/Paskirtoji saugumo institucija (PSI) - vyriausybės institucija, atsakinga už savo šalies įslaptintos informacijos apsaugą.

Informaciją parengusi Šalis - KI/PSI atstovaujama, įslaptintą informaciją parengusi Šalis.

Informaciją gaunanti Šalis - KI/PSI atstovaujama Šalis, kuriai siunčiama arba perduodama įslaptinta informacija.

2. Lietuvos Respublikoje įslaptinta informacija žymima: KONFIDENCIALIAI (CONFIDENTIAL), SLAPTAI (SECRET), VISIŠKAI SLAPTAI (TOP SECRET).

Estijos Respublikoje įslaptinta informacija žymima: KONFIDENSIAALNE (CONFIDENTIAL), SALAJANE (SECRET), TÄIESTI SALAJANE (TOP SECRET).

3. Estijos Respublika Lietuvos Respublikos įslaptintą informaciją, pažymėtą KONFIDENCIALIAI, saugos kaip Estijos Respublikos įslaptintą informaciją, žymimą KONFIDENSIAALNE, Lietuvos Respublikos įslaptintą informaciją, pažymėtą SLAPTAI, - kaip Estijos Respublikos įslaptintą informaciją, žymimą SALAJANE, ir Lietuvos

Respublikos įslaptintą informaciją, pažymėtą VISIŠKAI SLAPTAI, - kaip Estijos Respublikos įslaptintą informaciją, žymimą TÄIESTI SALAJANE.

4. Lietuvos Respublika Estijos Respublikos įslaptintą informaciją, pažymėtą KONFIDENSIAALNE, saugos kaip Lietuvos Respublikos įslaptintą informaciją, žymimą KONFIDENCIALIAI, Estijos Respublikos įslaptintą informaciją, pažymėtą SALAJANE, - kaip Lietuvos Respublikos įslaptintą informaciją, žymimą SLAPTAI, ir Estijos Respublikos įslaptintą informaciją, pažymėtą TÄIESTI SALAJANE, - kaip Lietuvos Respublikos įslaptintą informaciją, žymimą VISIŠKAI SLAPTAI.

5. Įslaptintą informaciją parengusios Šalies prašymu įslaptintą informaciją gaunanti Šalis pakeis ar panaikins informacijos klasifikacinę kategoriją. Apie įslaptinimo klasifikacijos kategorijos pakeitimą ar panaikinimą informaciją gaunančiai Šaliai pranešama per šešias savaites nuo įslaptinimo klasifikacinės kategorijos pakeitimo ar panaikinimo datos.

6. Iki įsigalios ši Sutartis, visa siunčiama ar perduodama įslaptinta informacija saugoma laikantis šios Sutarties nuostatų.

2 straipsnis

Šalių nacionaliniai įsipareigojimai

1. Vadovaudamosi nacionaline teise, Šalys įsipareigoja imtis visų reikiamų veiksmų, kad būtų apsaugota pagal šią Sutartį perduodama įslaptinta informacija arba su kuria susipažinti teisę gauna Sutarties dalyvis remiantis sutartimi, susijusia su įslaptinta informacija. Prireikus įslaptintą informaciją parengusi Šalis gali prašyti įslaptintą informaciją gaunančią Šalį suteikti gautai informacijai aukštesnę nei nurodyta įslaptinimo klasifikacinę kategoriją.

2. Susipažinti su įslaptinta informacija gali tik tokį leidimą turintys asmenys. Leidimas susipažinti su įslaptinta informacija išduodamas tik tiems asmenims, kurių patikimumo statusą nustatyta tvarka yra patikrinusios ir kuriems leidimą susipažinti su įslaptinta informacija yra išdavusios tikrinamo asmens šalies kompetentingos institucijos. Nė vienam asmeniui teisė naudotis įslaptinta informacija nesuteikiama dėl jo rango, einamų pareigų ar turimo patikimumo statuso. Teisė naudotis įslaptinta informacija gali būti suteikta tik tiems asmenims, kuriems ji reikalinga jų pareigoms atlikti.

3. Šalys neperduos gautos įslaptintos informacijos trečiosios šalies institucijoms ar subjektams be išankstinio PSI, kuri suteikė informacijos slaptumo klasifikacinę kategoriją, raštiško sutikimo. Tokia įslaptinta informacija gali būti naudojama tik nurodytam tikslui.

3 straipsnis

Įslaptintos sutartys

1. Jeigu Šalis rengiasi sudaryti su įslaptinta informacija susijusią sutartį su sutarties dalyviu, reziduojančiu kitos Šalies valstybės teritorijoje, arba su kitos Šalies sutarties dalyviu, reziduojančiu priimančiosios Šalies valstybės teritorijoje, prieš tai ji turi gauti tos kitos Šalies KI garantiją, kad būsimas sutarties dalyvis turi saugumo tarnybos išduotą patikimumo statusą, atitinkantį reikalaujamą informacijos įslaptinimo klasifikacinę kategoriją, ir kad jis yra įvykdęs atitinkamus saugumo susitarimus dėl įslaptintos informacijos apsaugos užtikrinimo. Pateikiamoje garantijoje, be kita ko, turi būti laiduojama, kad saugumo tarnybos patikrinto sutarties dalyvio susitarimai dėl apsaugos atitinka valstybės nacionalinius įstatymus, reglamentuojančius įslaptintos informacijos apsaugą, ir kad šiuos susitarimus kontroliuoja KI.

2. PSI, atsakinga už sutarties dalyvį, turi užtikrinti, kad visai įslaptintai informacijai, perduotai kitos Šalies sutarties dalyviui arba parengtai vykdant sutartį, būtų suteikta klasifikacinė kategorija. PSI, atsakingos už sutarties dalyvį, prašymu kitos Šalies PSI pateikia pastarajai įslaptintos informacijos saugumo reikalavimų sąrašą. Kitos Šalies PSI taip pat pateikia PSI, atsakingai už sutarties dalyvį, pranešimą, kuriame teigiama, kad sutarties dalyvis įsipareigoja laikytis nacionalinių įstatymų, reglamentuojančių įslaptintos informacijos apsaugą. Kitos Šalies PSI pateikia atitinkamą pranešimą sutarties dalyvio PSI apie jo įsipareigojimą saugoti įslaptintą informaciją.

3. Sutarties dalyvio PSI raštiškai patvirtina apie prašytą saugumo reikalavimų sąrašo gavimą ir šį sąrašą siunčia sutarties dalyviui.

4. Sutarties dalyvio PSI turi visais atvejais garantuoti, kad sutarties dalyvis su slaptai saugotina sutarties medžiagos dalimi elgsis taip kaip su jo valstybės įslaptinta informacija, vadovaudamasis kvalifikacine kategorija, nustatyta saugumo reikalavimų sąraše.

5. Tuo atveju, jei PSI patvirtintų įslaptintą subrangos sutartį, atitinkamai taikomos šio straipsnio 2 ir 4 dalys.

6. Šalys užtikrins, kad įslaptinta sutartis bus sudaryta arba kad darbas, numatytas įslaptintose sutarties dalyse, bus pradėtas tik po to, kai sutarties dalyvis įgyvendins saugumo priemones.

4 straipsnis

Dokumentų vertimas, kopijavimas ir naikinimas

1. Dokumentus, kuriuose yra informacijos, pažymėtos „VISIŠKAI SLAPTAI", leidžiama versti ir kopijuoti tik gavus informaciją parengusios Šalies PSI raštišką leidimą.

2. Visą įslaptintą informaciją verčia ir dokumentus kopijuoja asmenys, kurių *patikimumo statusas* atitinka šios Sutarties 2 straipsnio reikalavimus. Šie vertimai ir dokumentų kopijos žymimi atitinkamomis slaptumo klasifikacinėmis kategorijomis. Vertimų ir dokumentų kopijų daroma tiek, kiek jų reikia oficialiems tikslams.

3. Įslaptinti dokumentai naikinami juos sudeginant, supjaustant ar susmulkinami taip, kad atkurti juose buvusios įslaptintos informacijos būtų neįmanoma.

4. Įslaptinta medžiaga sunaikinama neatpažįstamai arba modifikuojama taip, kad nebūtų galima rekonstruoti nei jos visos, nei atskirų jos dalių.

5. Paprastai dokumentai ir medžiaga, pažymėti „VISIŠKAI SLAPTAI", nenaikinami, bet grąžinami siuntėjui po to, kai pripažįstama, kad jie nereikalingi arba pasibaigęs jų galiojimo laikas.

5 straipsnis

Įslaptintos informacijos siuntimas ir perdavimas

1. Paprastai įslaptinta informacija iš vienos Šalies į kitą perduodama per diplomatines ar karines kurjerių tarnybas arba per gynybos atašė. Įslaptintą informaciją gaunanti Šalis patvirtina įslaptintos informacijos gavimo faktą ir, laikydamasi nacionalinių įslaptintos informacijos apsaugos įstatymų, perduoda ją gavėjui.

2. Paskirtosios saugumo institucijos turi teisę konkrečiu atveju, bendrai ar su nustatytais apribojimais išduoti leidimą įslaptintą informaciją perduoti kitu būdu, ne diplomatinių ar karinių kurjerių kanalais, jeigu šių kurjerių naudojimas sukels nepagrįstų problemų, susijusių su sutarties perdavimu ar įvykdymu.

3. Šio straipsnio 2 dalyje nurodytais atvejais būtina laikytis šių reikalavimų:

1) informacijos siuntėjui suteikiama teisė naudotis atitinkamos klasifikacinės kategorijos įslaptinta informacija;

2) informaciją parengusi Šalis turi savo įstaigoje pasilikti išsiunčiamos įslaptintos informacijos sąrašą, o vieną šio sąrašo egzempliorių įteikti gavėjui, kad šis jį perduotų PSI;

3) įslaptinta informacija supakuojama bei užantspauduojama pagal reikalavimus perduoti šalies viduje;

4) įslaptintos informacijos įteikimas patvirtinamas raštu.

4. Jeigu reikia perduoti didelį įslaptintos informacijos kiekį, kiekvienu konkrečiu atveju Paskirtosios saugumo institucijos turi abipusiai suderinti bei patvirtinti transporto priemones, gabenimo maršrutus ir apsaugos palydą.

5. Įslaptinta informacija elektroninėmis priemonėmis perduodama tik visiškai užšifruota (naudojant tam kriptografijos priemones ir įtaisus).

6 straipsnis

Vizitai

1. Jeigu vienos Šalies atstovams reikėtų suteikti teisę lankytis kitos Šalies įstaigose ar saugyklose, kai jų apsilankymas yra susijęs su galimybe gauti įslaptintą informaciją, tokia teisė turi būti suteikta tik oficialiais tikslais. Teisę apsilankyti šiose įstaigose ir saugyklose gali suteikti tik atitinkamos KI/PSI. Šie vizitai gali vykti gavus šalies, į kurios teritoriją vykstama, KI/PSI sutikimą.

2. Lankytojo prašyme nurodoma ši informacija:

1) lankytojo vardas, pavardė, gimimo data ir vieta, paso numeris;

2) lankytojo oficialus statusas, kartu nurodomas saugyklos, įmonės ar organizacijos, kuriai lankytojas atstovauja ar priklauso, pavadinimas;

3) pažymėjimas, kuriame nurodytas lankytojo patikimumo statusas;

4) vizito tikslas ir numatoma atvykimo bei išvykimo data;

5) saugyklos, įmonės ar organizacijos, kurioje bus lankomasi, pavadinimas ir adresas (jei reikia).

7 straipsnis

Pažeidimas ir kompromisas

1. Jeigu įslaptintos informacijos apsaugos taisyklių pažeidimas, kuris gali lemti kitos Šalies perduotos įslaptintos informacijos praradimą ar atskleidimą arba galimą jos praradimą ar atskleidimą, yra neišvengiamas, esant prielaidai, kad ji gali būti ar yra atskleista arba praradus įslaptintą informaciją vienu ar kitu būdu, apie tai būtina nedelsiant pranešti kitai Šaliai.

2. Įslaptintos informacijos apsaugos taisyklių pažeidimų nustatymą ir tyrimą atlieka vadovaudamasi nacionaliniais teisės aktais su tuo susijusi Šalis. Tyrimo rezultatai kaip galima greičiau turi būti pranešami kitai Šaliai.

8 straipsnis

Išlaidos

Vienos Šalies išlaidų, susijusių su šios Sutarties įgyvendinimu, kita Šalis neturi kompensuoti.

9 straipsnis

Kompetentingos institucijos

Šios Sutarties tikslais Šalių kompetentingos institucijos yra šios:

1) Estijos Respublikoje:

Nacionalinio saugumo koordinatoriaus biuras

(Bureau of National Security Co-ordinator)

Lossi Plats 1A

EE-15161 Tallinn

Estijos Respublika;

2) Lietuvos Respublikoje:

Lietuvos Respublikos paslapčių apsaugos koordinavimo komisija

(Commission for Secrets Protection Co-ordination)

Vytenio g. 1

LT-2600 Vilnius

Lietuvos Respublika.

10 straipsnis

Baigiamosios nuostatos

1. Ši Sutartis įsigalioja tą dieną, kai Šalys pasikeičia notomis apie vidaus teisės reikalavimų, būtinų, kad ši Sutartis įsigaliotų, įvykdymą.

2. Ši Sutartis sudaroma neapibrėžtam laikotarpiui.

3. Visus nesutarimus dėl šios Sutarties aiškinimo ar vykdymo Šalys sprendžia derybomis.

4. Šios Sutarties pakeitimai gali būti daromi Šalių abipusiu sutikimu.

5. Kiekviena iš Šalių turi teisę nutraukti šią Sutartį apie tai prieš šešis mėnesius pranešdama raštu. Nepaisant šios Sutarties nutraukimo, visa pagal šią Sutartį perduota arba sutarties dalyvio parengta įslaptinta informacija, vadovaujantis šios Sutarties nuostatomis, laikoma įslaptinta tol, kol to reikalauja jai suteikta įslaptinimo klasifikacinė kategorija.

6. KI ir (ar) PSI gali sudaryti papildomų sutarčių ar susitarimų remiantis šia Sutartimi.

SUDARYTA ..... dviem egzemplioriais estų, lietuvių ir anglų kalbomis, kurių kiekvienas turi vienodą teisinę galią. Iškilus nesutarimų, pirmenybė teikiama tekstui anglų kalba.

ESTIJOS RESPUBLIKOS
VYRIAUSYBĖS VARDU

LIETUVOS RESPUBLIKOS
VYRIAUSYBĖS VARDU

[TRANSLATION - TRADUCTION]

ACCORD ENTRE LE GOUVERNEMENT DE LA RÉPUBLIQUE D'ESTONIE ET LE GOUVERNEMENT DE LA RÉPUBLIQUE DE LITUANIE RELATIF À LA PROTECTION MUTUELLE DES INFORMATIONS CLASSIFIÉES

Le Gouvernement de la République d'Estonie et le Gouvernement de la République de Lituanie (ci-après dénommés les "Parties"),

Souhaitant renforcer la coopération politique, militaire, économique, juridique, scientifique et technologique entre les Parties ;

Coordonnant les efforts en direction de l'OTAN ;

Prenant note que la coopération peut exiger l'échange d'informations classifiées entre les Parties ;

Voulant assurer la protection des informations classifiées ;

Sont convenus de ce qui suit :

Article 1. Dispositions générales

1. Aux fins du présent Accord les expressions :

Information classifiée" signifie toute pièce classifiée, qu'elle soit orale ou visuelle, qu'elle ait été transmise par des moyens électriques ou électroniques qui ne peut être divulguée dans l'intérêt de la sécurité nationale et qui bénéficie d'une protection contre compromis.

Matière classifiée" s'entend de tout objet, machinerie ou équipement ou armes manufacturés ou en cours de fabrication ou document.

Document classifié" s'entend de tout support dans lequel figurent des informations classifiées y compris mais non exclusivement des lettres, des notes, des minutes, des rapports, des memoranda, des signaux, des messages, des croquis, des photos, des films, des cartes, des tableaux, des carnets, des stencils, des carbones, des rubans de machine à écrire, des disquettes etc. ou toute autre forme d'information enregistrée.

Contractant" s'entend d'une personne physique ou morale ayant la capacité légale ou juridique de signer des contrats.

Contrat classifié" désigne tout contrat qui prévoit des dispositions pour l'utilisation d'informations classifiées.

Autorité compétente" (CA), Autorité désignée pour la sécurité (DSA) signifie toute autorité gouvernementale responsable de la sécurité de l'information dans chacun des pays.

Partie d'origine" s'entend de la Partie d'où provient l'information classifiée (telle que représentée par CA/DSA).

Partie qui reçoit" signifie Partie à laquelle l'information classifiée est transmise ou transférée (telle que représentée par CA/DSA).

2. Pour la République de Lituanie, l'information classifiée est désignée par KONFIDENCIALIAI (CONFIDENTIEL), SLAPTAI (SECRET), VISISKAI SLAPTAI (ULTRA CONFIDENTIEL). Pour la République d'Estonie, l'information classifiée est désignée par KONFIDENSIAALNE (CONFIDENTIEL), SALAJANE (SECRET), TAIESTI SALAJANE (ULTRA CONFIDENTIEL).

3. La République d'Estonie protégera l'information lituanienne classifiée KONFIDENCIALIAI comme l'information estonienne KONFIDENSIAALNE, l'information lituanienne classifiée SLAPTAI comme

l'information estonienne SALAJANE et l'information lituanienne classifiée VISISKAI SLAPTAI comme l'information estonienne TAIESTI SALAJANE.

4. La République de Lituanie protégera l'information classifiée estonienne KONFIDENSIAALNE comme l'information lituanienne KONFIDENCIALIAI, l'information estonienne SALAJANE telle que l'information lituanienne SLAPTAI et l'information estonienne classifiée TAIESTI SLAJANE telle que l'information lituanienne VISISKAI SLAPTAI.

5. Le niveau de classification sera modifié ou révoqué par la Partie qui reçoit à la demande de la partie d'origine. La modification ou la révocation de la classification doit être notifiée à la Partie qui reçoit dans un délai de six semaine à partir de la date de la modification ou de la révocation de la classification.

6. Toutes les informations classifiées transmises ou transférées avant le présent Accord n'entre en vigueur seront protégées conformément à ses dispositions.

Article 2. Les responsabilités nationales

1. Les Parties doivent prendre dans le cadre de leur législation nationale toutes les mesures nécessaires pour assurer la protection des informations classifiées qui doit être transmise, conformément au présent Accord et à laquelle un mandataire a accès selon les termes d'un contrat portant sur des informations classifiées. Dans certaines occasions, la Partie d'origine peut demander à la Partie qui reçoit d'accorder à l'information un niveau de protection plus élevé que celui indiqué.

2. Seules les personnes autorisées peuvent avoir accès aux informations classifiées. L'autorisation n'est accordée qu'aux personnes ayant subi un examen de sécurité et qui a été autorisée par les autorités de son pays à avoir accès à des informations classifiées. L'accès n'est accordé qu'aux personnes qui ont besoin de ces informations pour exécuter leurs tâches officielles.

3. Les Parties ne peuvent pas communiquer les informations classifiées aux autorités ou à des organisations d'une tierce partie sans l'approbation écrite du DSA qui a fixé une classification de sécurité. De telles informations classifiées ne peuvent être utilisées que pour des buts spécifiques.

Article 3. Contrats classifiés

1. La Partie qui a l'intention de conclure un contrat relatif à des informations classifiées avec un mandataire qui réside sur le territoire de l'autre Partie contractante ou avec un man-

dataire de l'autre Partie qui réside sur le territoire doit obtenir du CA la garantie que le mandataire proposé répond aux critères de sécurité correspondant au niveau de classification et a mis en oeuvre les mesures de sécurité appropriées pour assurer la protection de l'information classifiée. Cette garantie comporte l'obligation de s'assurer que les mesures de sécurité concernant le mandataire correspondent à la législation nationale relative à la protection de l'information classifiée et que ces mesures sont supervisées par le CA.

2. Il incombe aux autorités désignées pour la sécurité (DSA) du mandataire de s'assurer que toutes les pièces classifiées qui ont été remises au mandataire de l'autre Partie dans le cadre d'un contrat sont classifiées du point de vue de la sécurité. A la demande de l'autorité (DSA) du mandataire, l'autorité de l'autre Partie doit fournir une liste des mesures de sécurité. L'autorité de l'autre Partie doit informer l'autorité du mandataire que ce dernier s'engage à observer les dispositions de la législation nationale sur la protection des informations classifiées. L'autorité de l'autre Partie doit transmettre une notification appropriée de l'obligation du mandataire de protéger l'information classifiée de l'autorité du mandataire

3. Les autorités compétentes de la Partie destinataire accusent par écrit réception de cette liste qu'elle remet au destinataire.

4. Les autorités compétentes de la Partie destinataire s'assurent que le mandataire traite les pièces classifiées de l'autre Partie contractante comme s'il s'agissait de pièces classifiées de son propre état conformément à leur classification et conformément au niveau de classification fixé sur la liste.

5. Si le DSA approuve un contrat classifié, les paragraphes 2 et 4 du présent article s'appliquent en conséquence.

6. Les Parties contractantes s'assurent que les contrats concernant les informations classifiées ne soient conclus et que le travail concernant les Parties de ces contrats qui exigent des mesures de protection ne commence tant que le mandataire n'a pas pris les dispositions nécessaires en temps utile pour assurer leur secret.

Article 4. Traduction, reproduction et destruction

1. Les documents portant la mention "ULTRA CONFIDENTIEL" ne peuvent être traduits ou copiés qu'avec la permission écrite du DSA de la Partie d'origine.

2. Les traductions et les reproductions des informations classifiées ne peuvent être effectuées que par les personnes qui ont obtenu des garanties de sécurité conformément à l'article 2 du présent Accord. Les traductions et les reproductions doivent être revêtues de la classification de sécurité appropriée. Le nombre de copies de ces traductions et de ces reproductions doit être limité au nombre officiel requis.

3. Les documents classifiés doivent être détruits par incinération, broyage ou mis au pilon afin de prévenir la reconstitution des informations classifiées qui y figurent.

4. Le matériel classifié doit être détruit totalement afin de prévenir la reconstitution en totalité ou en partie des informations qui y figurent.

5. Les documents "ULTRA CONFIDENTIELS" ne doivent pas être détruits mais être retournés à ceux qui l'ont expédiés s'ils ne sont plus nécessaires ou à l'expiration de leur validité.

Article 5. Transfert d'informations classifiées

1) Les informations classifiées sont remises par l'une des Parties contractantes par courrier diplomatique ou militaire. Les autorités compétentes accusent réception des informations classifiées et les remettent au destinataire conformément à leur réglementation nationale relative à la protection des informations classifiées.

2) Les autorités compétentes peuvent convenir dans certains cas, de manière générale ou dans certaines conditions, que les informations classifiées peuvent être transmises conformément aux dispositions du paragraphe 3 par des voies autres que les courriers diplomatiques ou militaires dans la mesure ou l'acheminement par ce moyens pourrait poser des difficultés excessives pour le transport.

3) Dans les cas visés au paragraphe 2 du présent article :

Le transporteur doit être habilité à avoir accès aux informations classifiées dans une catégorie de classification comparable ;

L'organe qui envoie les informations doit conserver une liste des informations transmises et cette liste doit être remise au destinataire afin qu'il la transmette aux autorités compétentes ;

Les informations classifiées doivent être emballées conformément aux conditions prescrites pour l'envoi des informations nationales ;

La remise des informations classifiées se fait contre un accusé de réception ;

Le transporteur doit être muni d'une pièce d'identité de courrier établie par l'autorité de la sécurité compétente de l'agence d'où proviennent les informations ou qui les reçoivent.

4) Pour le transport d'informations classifiées dont le volume est important, les autorités compétentes déterminent les conditions et l'itinéraire du transport ainsi que les mesures de protection pour son accompagnement.

5. La transmission électronique des informations classifiées doit être entièrement codée (par l'utilisation d'une machine à coder).

Article 6. Visites

1) L'autorisation de visites ne peut être accordée qu'aux représentants d'une Partie qui doivent avoir accès pour des raisons officielles à des informations classifiées stockées dans des établissements et les installations de l'autre Partie. L'autorisation de visiter ces installations ne peuvent être accordées que par les CA/DSA respectifs des deux Parties. Avant la visite, l'approbation du CA/DSA du pays hôte est nécessaire.

2) La demande de visite doit inclure les informations suivantes :

Le nom du visiteur, son prénom, le lieu et sa date de naissance et le numéro de son passeport ;

Statut officiel du visiteur ainsi que le nom de l'établissement, la compagnie et l'organisation que le visiteur représente ;

Certificat indiquant le niveau de garantie de sécurité du visiteur ;

But de la visite et date de l'arrivée et du départ ;

Nom et adresse de l'établissement, compagnie et organisation à visiter.

Article 7. Infraction aux règlements concernant la protection des informations classifiées

1) Si la divulgation non sanctionnée d'informations classifiées contrairement aux règlements n'est pas à exclure mais est présumée ou constatée, elle doit être signalée immédiatement à l'autre Partie contractante.

2) Les infractions aux règlements concernant la protection des informations classifiées font l'objet d'enquêtes conformément à la législation nationale de la Partie concernée. Les résultats doivent être communiqués à l'autre Partie le plus tôt possible.

Article 8. Coûts

Les coûts encourus par l'une des Parties contractantes pour appliquer les mesures de sécurité ne sont pas remboursés par l'autre Partie contractante.

Article 9. Les autorités compétentes

1. Pour la mise en oeuvre du présent Accord, les autorités compétentes sont:

Pour la République d'Estonie :

Bureau du coordonnateur pour la sécurité

Lossi Plats 1A

EE-15161 Tallinn

République d'Estonie

Pour la République de Lituanie :

Commission pour la coordination de la protection des secrets

Vytenio g., 1,2600 Vilnius

République de Lituanie

Article 10. Dispositions finales

1) Le présent Accord entre en vigueur à la date de l'échange de notes indiquant que les procédures légales néeessaires à cette fin ont été accomplies.

2) Le présent Accord et conclu pour une période indéfinie.

3) Tout différend résultant de l'interprétation ou de l'application du présent Accord est résolu à l'amiable après consultations entre les Parties.

4) Les amendements au présent Accord sont effectués avec le consentement mutuel des Parties ;

5) Chacune des Parties peut dénoncer l'accord par écrit avec un préavis de six mois. En cas de dénonciation, les informations classifiées remises ou envoyées par le mandataire d'un contrat sur la base du présent Accord continuent de s'appliquer conformément au paragraphe 1 de l'article 2 aussi longtemps que stipulé par le marquage.

6) Les autorités compétentes peuvent conclure des accords supplémentaires ou effectuer des arrangements conformes au présent Accord.

Fait à Tartu le 26 mai 2000 en deux textes originaux en estonien, lituanien et anglais ; en cas de divergence d'interprétation, le texte anglais prévaudra.

Pour le Gouvernement de la République d'Estonie :

[TOOMAS HENRIK ILVES]

Pour le Gouvernement de la République de Lituanie :

[ALGIRDAS SAUDARGAS]