No. 37435

Estonia
and
Italy

Agreement between the Government of the Republic of Estonia and the Government of the Italian Repnblic for the mutual protection of classified information. Tallinn, 23 November 2000

Entry into force: *8 March 2001, in accordance with article 15*

Authentic texts: *Estonian and Italian*

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

Estonie
et
Italie

Accord entre le Gouvernement de la République d'Estonie et le Gouvernement de la République d'Italie relatif à la protection mutuelle des informations classifiées. Talliun, 23 novembre 2000

Entrée en vigueur : *8 mars 2001, conformément à l'article 15*

Textes autheutiques : *estonien et italien*

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

[ESTONIAN TEXT — TEXTE ESTONIEN]

Eesti Vabariigi valitsuse ja Itaalia Vabariigi valitsuse julgeolekukokkulepe salastatud teabe vastastikuse kaitse osas

1. Eesti Vabariigi valitsus ja Itaalia Vabariigi valitsus, edaspidi "lepingupooled", eesmärgiga vastastiku kaitsta salastatud teavet, mida vahetatakse otse või kummagi lepingupoole valitsemisalas salastatud teabega tegeleva haldusüksuse või eraettevõtte kaudu, valitsustevaheliste või mistahes muud riiklikku järelvalvet nõudvate lepingute raamistikus, leppisid kokku järgnevas:

ARTIKKEL 1
KOHALDAMINE

1. Kokkulepe on aluseks igasugusele tegevusele, mis sisaldab salastatud teabe vahetamist, järgmiste valdkondade kohta:

a) lepingupooltevaheline koostöö riigikaitse ja muudes küsimustes, mis on seotud riikliku julgeolekuga;

b) koostöö, ühisettevõtted, lepingud ning muud lepingupoolte asutuste ja/või eraettevõtete suhted, mis on seotud riigikaitse ja muude küsimustega, mis on seotud riikliku julgeolekuga;

c) varustuse ja oskusteabe müümine ühelt lepingupoolelt teisele, mis on seotud riigikaitse ja riikliku julgeolekuga.

ARTIKKEL 2
MÕISTED

Kokkuleppes tähendab:

- **salastatud teave**

a) "salastatud teave" tähendab punktides b) ja c) määratletud salastatud dokumenti ja materjali või tegevust, teavet või mistahes muud asja, mille suhtes on kasutatud salastatuse märgist;

b) "salastatud dokument" tähendab mistahes viisil salvestatud salastatud teavet, sõltumata tema vormist või füüsilistest omadustest, mis võib esineda kirjalikult või trükituna, andetöötluskaartidel, magnetlintidel, kaartidel, fotodel, joonistustel, joonistel, graveerimistel, visanditel, märkmetes, kopeerpaberil, kirjutusmasina lintidel, salvestistel (heli, video), kaasaskantava arvutustehnika eemaldatavas või püsimälus või muus vormis;

c) mõiste "salastatud materjal" hõlmab iga mehaaniliselt toodetud või käsitsi tehtud masina, masina prototüübi, mis tahes varustuse, relva või relvasüsteemi valmis või tootmisjärgus osist, millel on salastatusmärge;

d) "salastatusmärge" on üks salastatuse tasemetest, mis on toodud artiklis 6.

- **lepingu**

kahe- või mitmepoolset kokkulepet, milles määratletakse lepingupooltevahelised õigused ja kohustused;

- **salastatud leping**

kahe- või mitmepoolset kokkulepet, milles määratletakse lepingupoolte vahelised õigused ja kohustused, mis sisaldab salastatud teavet või mille sisu on sellega seotud;

- **lepingupartner**

füüsilist või juriidilist isikut, kellel on juriidiline õigus lepingut sõlmida;

- **julgeolekunõuete rikkumine**

riiklikke julgeolekualaseid õigusakte rikkuvat tegevust või tegevusetust, mille tulemusel võib salastatud teave lekkida või selle salastatus ohtu sattuda;

- **teabeleke**

kogu salastatud teabe või selle osa sattumist isiku, asutuse või riigi kätte, kellel puudub asjakohane juurdepääsuluba või salastatud teabele juurdepääsu õigus, või nimetatute poolt sellise teabe edastamise ohtu;

- **juurdepääsuluba**

isiku lojaalsuse ja usaldusväärsuse suhtes teostatud julgeolekukontrolli tulemusel langetatud positiivne otsus selle kohta, et eespool nimetatul on salastatud teabele juurdepääsu õigus ja ta on võimeline sellist teavet töötlema kuni teatud salastatuse tasemeni kooskõlas asjakohaste riiklike julgeolekualaste õigusaktidega;

- **rajatise juurdepääsuluba**

riikliku või eraettevõtte rajatise suhtes teostatud julgeolekukontrolli tulemusel langetatud positiivne otsus selle kohta, et eespool nimetatus on tagatud organisatoorsed ja füüsilise julgeoleku alased meetmed salastatud teabe teatud tasemel käsitlemiseks kooskõlas asjakohaste riiklike julgeolekualaste õigusaktidega;

- **teadmisvajadus**

et juurdepääs salastatud teabele võidakse tagada ainult sel juhul, kui seda taotleval isikul on tõestatud, tema ametiülesannetest tingitud teadmisvajadus, mille kontekstis teave vastuvõtvale lepingupoolele edastati.

ARTIKKEL 3
SALASTATUD TEABE KAITSE

1. Lepingupool võtab teise lepingupoolega suhtlemise või temaga sõlmitud kokkuleppe tulemusel edastatava, vastuvõetava, toodetava või täiustatava salastatud teabe kaitseks kohaseid meetmeid vastavalt oma riigi õigusaktidele, korraldustele ja praktikale. Lepingupool tagab kogu edastatavale, vastuvõetavale, toodetavale või täiustatavale salastatud teabele samasuguse kaitse nagu oma salastatud teabele, mis on kokkuleppe artiklis 6 määratletu kohaselt samal salastatuse tasemel.
2. Teavet vastuvõttev lepingupool ja/või tema asutused ei tohi saadud teabel kasutada madalama salastatuse taseme märgist või alandada salastatuse taset selle edastanud lepingupoole kirjaliku nõusolekuta. Teabe edastanud lepingupool teavitab selle vastuvõtnud lepingupoolt vahetatud teabe salastatuse tasemete muutustest.

3. Juurdepääs salastatud teabele ning kohtadele ja ehitistele, kus toimub salastatud tegevus või kus hoitakse salastatud teavet, on piiratud vaid juurdepääsuloaga isikutega, kellel on tema ametiülesannetest või töökohast tingitud teadmisvajadus.
4. Lepingupool valvab julgeolekualaste õigusaktide täitmise järele ning tema jurisdiktsioonile alluvates, teise lepingupoole salastatud teavet valdavates, täiustavates, tootvates, koostavates ja/või kasutavates asutustes ja ehitistes toimuva tegevuse järele, tehes muu hulgas ka inspektsioone.
5. Lepingupool ei tohi edastada teiselt lepingupoolelt saadud salastatud teavet kolmandatele riikidele või organisatsioonidele ilma teise lepingupoole nõusolekuta.
6. Lepingupool ei tohi käesolevat kokkulepet kasutada sellise salastatud teabe omandamiseks, mida teine lepingupool on saanud kolmandalt riigilt või organisatsioonilt.

ARTIKKEL 4
JUURDEPÄÄSULOAD

1. Lepingupool tagab, et iga isik, kes oma ametiülesannete tõttu vajab juurdepääsu salastatud teabele, mis on salastatud vähemalt konfidentsiaalse tasemega, omab vastavat ja kehtivat juurdepääsuluba, mille on andnud riigi julgeolekuasutus või muu pädev asutus.
2. Isiku suhtes, kellele antakse juurdepääsuluba salastatud teabele, teostatakse julgeolekukontroll, mille käigus määratakse kindlaks antud isiku usaldusväärsus ja lojaalsus riigile.
3. Taotluse korral abistavad Lepingupooled teineteist juurdepääsulubade ja rajatiste juurdepääsulubade väljastamisel oma siseriikliku seadusandluse raames pädevate riiklike julgeolekuasutuste kaudu.

ARTIKKEL 5
TEABE EDASTAMINE KOLMANDALE RIIGILE VÕI ORGANISATSIOONILE

1. Käesoleva kokkuleppe raames teiselt poolelt saadud salastatud teabe edastamine kolmandale riigile või organisatsioonile toimub edastava lepingupoole vahendite ja toimingute kohaselt. Edastav lepingupool võib kehtestada lisakitsendused salastatud teabe edastamisele.
2. Lepingupool võib teiselt lepingupoolelt saadud salastatud teavet kasutada ainult kindlaksmääratud eesmärgil.

ARTIKKEL 6
SALASTATUSE TASEMED

1. Käesoleva kokkuleppe raames vahetatava salastatud teabe salastatuse tasemete vastavused on järgmised:

EESTI	ITAALIA
TÄIESTI SALAJANE	SEGRETISSIMO
SALAJANE	SEGRETO
KONFIDENTSIAALNE	RISERVATISSIMO

2. Lepingupool tagab, et teave, mis on märgistatud vastavalt:

EESTI	ITAALIA
AVALDAMISELE MITTEKUULUV ja/või AMETKONDLIK	RISERVATO

on kaitstud vastavalt lepingupoolte siseriiklikule seadusandlusele.

ARTIKKEL 7

PÄDEVAD ASUTUSED

1. Käesoleva kokkuleppe kõigi valdkondade rakendamise ja selle järelevalve eest vastutavad pädevad julgeolekuasutused on:

EESTI VABARIIGIS:	ITAALIA VABARIIGIS:
Koordinatsioonidirektori büroo	Presidenza del Consiglio dei Ministri
Riigikantselei	Autorità Nazionale per la Sicurezza
Stenbocki maja	CESIS - III°Reparto U.C.Si.
Rahukohtu 3	Via della Pineta Sacchetti, n. 216
15161 Tallinn	00168 Roma
E E S T I	I T A L I A

Lepingupool tagab, et tema pädev julgeolekuasutus täidab kokkulepet täpselt.

2. Oma riigi pädevuse piires valmistavad mõlemad julgeolekuasutused ette ja annavad mis tahes lepingupooltevahelise kokkuleppe tulemusel vahetatava salastatud teabe kaitseks vajalikke julgeolekueeskirju ning kontrollivad nende täitmist.

3. Teise lepingupoole pädeva julgeolekuasutuse taotluse korral annab lepingupoole julgeolekuasutus talle infot oma julgeolekukorralduse ja -toimingute kohta, et võimaldada julgeolekustandardite võrdlemist ja samaväärsena hoidmist ning soodustada kummagi riigi volitatud ametiisikute vastastikuseid visiite. Sellised visiidid tuleb lepingupooltel omavahel kooskõlastada.

ARTIKKEL 8

VISIIDID

1. Lepingupool lubab teise lepingupoole esindajal külastada oma salastatud teabe täiustamise, töötlemise või säilitamise või salastatud projektide ja/või lepingute teostamise kohti, kui külastatava lepingupoole pädev julgeolekuasutus on andnud

selleks eelneva kirjaliku loa. Selline luba antakse ainult sellisele isikule, kes on läbinud julgeolekukontrolli ja kellel on teadmisvajadus.

2. Visiitidega seotud protseduurid lepitakse kokku vastavalt artiklis 7 toodud Lepingupoolte pädevate julgeolekuasutuste poolt.
3. Mõlemad lepingupooled garanteerivad külastajate isikuandmete kaitse vastavalt kehtivale siseriiklikule seadusandlusele.

ARTIKKEL 9
TÖÖSTUSJULGEOLEK

1. Kui lepingupool ja/või tema asjaomane, artiklis 1 nimetatud valdkonnaga tegelev ametkond või asutus sõlmis teise lepingupoole territooriumil tööde tegemiseks või projektide rakendamiseks salastatud teavet sisaldava või sellise teabega seotud lepingu, haldab sellist salastatud teavet oma julgeolekustandardite ja -nõuete kohaselt see lepingupool, kelle riigis lepingus ettenähtud töid tehakse või projekte rakendatakse.
2. Enne olemasolevale või tulevasele lepingupartnerile teiselt lepingupoolelt saadud salastatud teabe edastamist, peab teavet vastuvõttev lepingupool:

a) tagama, et selline lepingupartner ning selle asutused on võimelised salastatud teavet nõuetekohaselt kaitsma;
b) andma lepingupartnerile asjakohase rajatise juurdepääsuloa;
c) andma asjakohased isiku juurdepääsuload kõigile töötajatele, kelle ametiülesanded eeldavad juurdepääsu salastatud teabele;
d) informeerima kõiki asjakohase juurdepääsuloaga töötajaid nende kohustusest kaitsta salastatud teavet vastavalt kehtivatele seadustele.

3. Lepingupoolte asutuste ja/või eraettevõtete vahel sõlmitud salastatud lepingud peavad sisaldama asjakohast julgeolekut käsitlevat osa ja teabe salastamise juhiseid, mis põhinevad käesoleval kokkuleppel.

Selle riigi, kus salastatud lepingu järgset tööd tehakse, pädev julgeolekuasutus vastutab lepingu kaitseks julgeolekumeetmete ettekirjutamise ning nende meetmete võtmise eest, tuginedes oma salastatud lepingute kaitset reguleerivatele standarditele ja nõuetele.

Nimekiri potentsiaalsetest salastatud lepingutest huvitatud alltöövõtjatest pakub lepingupartner enne temaga lepingu sõlmimist välja pädevale julgeolekuasutusele heakskiitmiseks. Kui taotleja on heaks kiidetud, täidab ta alltöövõtjana samu julgeolekualaseid kohustusi, mis on pandud lepingupartnerilegi.

4. Iga salastatud projekti, lepingu, kokkuleppe või alltöövõtulepingu kohta saadetakse eelteatis selle lepingupoole, kus hakatakse projekti rakendama, pädevale julgeolekuasutusele.

   Kaks koopiat iga salastatud lepingu julgeolekut käsitlevast osast edastatakse selle riigi pädevale julgeolekuasutusele, kus salastatud lepingu järgset tööd tehakse või projekti rakendatakse.

5. Lepingupooled kaitsevad vahetatud salastatud informatsiooniga seoses olevaid autori-, tööstusteabe – patendid kaasa arvatud – ja muid õigusi.

ARTIKKEL 10
SALASTATUD TEABE EDASTAMINE

I. Üldjuhul edastavad lepingupooled salastatud teavet oma diplomaatiliste kanalite kaudu.

   Salastatud teavet võib vahetada ka kummagi lepingupoole pädevate julgeolekuasutuste poolt ametlikult määratud esinduste kaudu. Taotluse korral võib sellise volituse anda eriprojekti kaasatud tööstusettevõtte esindajale.

2. Suuremate salastatud esemete või suurema hulga salastatud teabe edastamine lepitakse pädevate julgeolekuasutuste poolt kokku iga juhtumi puhul eraldi.

3. Teisi heakskiidetud teabeedastusviise võib kasutada kokkuleppel kummagi pädeva julgeolekuasutusega.

ARTIKKEL 11
JULGEOLEKUNÕUETE RIKKUMINE

1. Kui salastatud teabe suhtes, mis on saadud teiselt lepingupoolelt või on tema poolt koostatud, on rikutud julgeolekunõudeid, mille tõttu tekib kindel või võimalik teabeleke, peab selle riigi pädev julgeolekuasutus, kus info lekib, informeerima teise lepingupoole pädevat julgeolekuasutust nii kiiresti kui võimalik ja läbi viima asjakohase uurimise.

   Taotluse korral teeb teine lepingupool temaga uurimise läbiviimisel koostööd.
2. Teist lepingupoolt teavitatakse igal juhul uurimise tulemustest ja talle saadetakse julgeolekunõuete rikkumise ulatust ja põhjusi kajastav kokkuvõte.

ARTIKKEL 12
KULUTUSED

1. Käesoleva kokkuleppe kasutusele võtmine ei too lepingupooltele endaga tavaliselt kaasa mingeid kulutusi.
2. Juhul kui kokkuleppega tekivad kulud, siis katab iga lepingupool nad ise vastavalt siseriiklikele õigusaktidele. Mingil juhul ei nõuta nende kulude hüvitamist teiselt lepingupoolelt.

ARTIKKEL 13
ERIMEELSUSTE LAHENDAMINE

1. Kokkuleppe rakendamise või tõlgendamisega seotud erimeelsused lahendatakse heatahtlikult lepingupooltevaheliste konsultatsioonide teel.

ARTIKKEL 14
MUUD KÜSIMUSED

1. Artiklite pealkirjad on mõeldud vaid viitamise lihtsustamiseks ning ei ole mõeldud ega ei või kasutada artiklite sisu kitsendamiseks või laiendamiseks.
2. Kumbki lepingupool ei oma õigust üle anda või muul moel loovutada oma õigusi ja kohustusi, mis on määratletud selle kokkuleppega, ilma teise lepingupoole kirjaliku nõusolekuta.
3. Lepingupool abistab teise lepingupoole isikuid nende teenistusülesannete täitmisel ja/või õiguste teostamisel vastavalt käesoleva kokkuleppe tingimustele, kui nad on tema riigis.
4. Vastavalt vajadusele peavad lepingupoolte pädevad julgeolekuasutused nõu selle lepingu täitmise spetsiifiliste tehniliste aspektide üle ja vastavalt vajadusele võivad kokku leppida täiendavate protokollide lisamises sellele lepingule juhtumite kaupa.

ARTIKKEL 15
LÕPPSÄTTED

1. Käesolev kokkulepe jääb kehtima piiramata ajaks ja jõustub esimesel päeval, mis järgneb sellele, mil mõlemad lepingupooled on saanud teiselt poolelt ametliku kinnituse, et pool on läbinud siseriiklikud kokkuleppe jõustamiseks vajalikud protseduurid.
2. Lepingupool võib selle igal ajal kirjaliku teatamise teel lõpetada. Sel juhul kaotab kokkulepe kehtivuse kuus kuud pärast seda, kui teine lepingupool on saanud kirjaliku lõpetamisteate.
3. Kumbki lepingupool teavitab teist lepingupoolt koheselt kõikidest muudatustes oma seadusandluses, mis võivad mõjutada salastatud teabe kaitsmist käesoleva kokkuleppe kohaselt. Sellisel juhul konsulteerivad lepingupooled omavahel arutamaks võimalikke muudatusi kokkuleppes. Samal ajal jätkub salastatud teabe kaitsmine vastavalt kokkuleppele, välja arvatud teavet edastava lepingupoole kirjalikul nõudmisel.

4. Vaatamata kokkuleppe lõppemisele, kaitstakse käesoleva kokkuleppe kohaselt edastatud salastatud teavet endiselt kooskõlas käesoleva kokkuleppe sätetega.
5. Kokkulepet võib igal ajal mõlema lepingupoole kirjalikul nõusolekul uuesti läbi vaadata, muuta või täiendada.
6. Kokkuleppe rakendamise vältel edastatud salastatud esemed ja/või teave tagastatakse kokkuleppe lõpetamise korral teisele lepingupoolele nii kiiresti kui võimalik. Salastatud teavet ja/ või esemeid, mida ei tagastata, kaitstakse vastavalt käesolevas kokkuleppes sätestatud korrale.

Käesoleva tõendamiseks kirjutasid mõlema riigi volitatud esindajad kokkuleppele alla.

Koostatud Tallinnas 23.11.00 kahes eksemplaris eesti ja itaalia keeles, mõlemad tekstid on võrdse jõuga.

Eesti Vabariigi valitsuse nimel

Itaalia Vabariigi valitsuse nimel

[ITALIAN TEXT — TEXTE ITALIEN]

Accordo di Sicurezza tra il Governo della Repubblica di Estonia ed il Governo della Repubblica Italiana per la reciproca tutela delle informazioni classificate

1. Il Governo della Repubblica di Estonia ed il Governo della Repubblica Italiana, di seguito chiamate Parti Contraenti, volendo garantire la reciproca tutela di tutte le informazioni classificate scambiate direttamente o tramite altre amministrazioni pubbliche o organizzazioni private poste sotto la giurisdizione delle Parti Contraenti o inserite in atti Governativi o che siano oggetto di atti pubblici, hanno concordato quanto segue:

ARTICOLO 1
APPLICABILITA'

1. Questo Accordo verrà applicato in ogni genere di attività volta allo scambio di informazioni classificate tra le parti Contraenti riguardanti le seguenti aree:

   a. cooperazione tra le Parti Contraenti concernenti la difesa nazionale ed ogni altra materia riguardante la sicurezza nazionale;

   b. cooperazione, joint ventures, contratti ed ogni altro rapporto tra enti pubblici e privati delle Parti Contraenti concernenti la difesa nazionale ed ogni altra materia riguardante la sicurezza nazionale;

   c. vendita di equipaggiamenti e di conoscenze tecniche tra una Parte Contraente e l'altra, connesse con la difesa e la sicurezza nazionale.

ARTICOLO 2
DEFINIZIONI

1. Ai fini di questo Accordo:

   ♦ il termine **"Informazione classificata"** significa:

   a. Per "informazione classificata" ciascun documento o materiale di cui al sottoparagrafo b. e c. sottospecificato, o qualsiasi atto, informazione, attività ed ogni altra cosa a cui è stata applicata una classifica di sicurezza;

   b. Per "documento classificato", ogni informazione classificata senza riguardo alla sua forma o caratteristica fisica, con l'inclusione, senza alcuna limitazione, di quella scritta o stampata, di elaborati e nastri, carte topografiche, fotografie, immagini, disegni, incisioni, schizzi, appunti, carta carbone e nastri

inchiostrati, o riproduzioni con ogni mezzo o procedimento, o suono, voce, registrazioni magnetiche o elettroniche o ottiche o video di qualsiasi forma ed equipaggiamento portatile ADP con disco fisso o estraibile;

c. Per "materiale classificato", qualsiasi oggetto o parte di macchinario, prototipo, equipaggiamento, arma, etc, meccanico o fatto a mano, costruito o in corso di costruzione, contrassegnato con una classifica di sicurezza;

d. per "classifica di sicurezza", una delle classifiche riportate al successivo art.6.

Contratto classificato significa:
un Accordo tra due o più Parti Contraenti al fine di stabilire diritti ed obblighi tra le Parti Contraenti, che contiene o prevede l'uso di informazioni classificate.
Contraente o sub-contraente significa:
una persona fisica o giuridica che abbia la capacità legale di sottoscrivere contratti.

Infrazione alla sicurezza significa:
un atto o una omissione contraria alle norme di sicurezza nazionali, il cui risultato possa mettere in pericolo o compromettere informazioni classificate.

Compromissione della sicurezza significa:
il fatto che la conoscenza di informazioni classificate sia stata passata, in tutto o in parte, a persone o enti o Paesi sprovvisti di un'adeguata abilitazione di sicurezza o autorizzazione a tale accesso, o quando ci sia stato rischio che questo avvenisse.

Abilitazione personale di Sicurezza significa:
il giudizio positivo derivante da una procedura di indagine finalizzata ad accertare la lealtà e l'affidabilita' di una persona sulla base della quale egli/ella potrà avere accesso e trattare informazioni classificate fino ad un determinato livello secondo le rispettive norme di sicurezza nazionale.

Abilitazione di Sicurezza di persone giuridiche significa:
il giudizio positivo derivante da una procedura di indagine finalizzata ad accertare la capacità fisica ed organizzativa di un ente pubblico e/o privato di trattare informazioni classificate ad un certo livello, in accordo con le rispettive leggi e regolamenti di sicurezza nazionale.

"Necessità di Conoscere" significa:
il principio secondo il quale l'accesso alle informazioni classificate può essere consentito soltanto a persona che abbia una oggettiva necessità di conoscere, conseguente al suo incarico, nel cui contesto l'informazione è stata rilasciata alla Parte Contraente che la riceve.

ARTICOLO 3
PROTEZIONE DELLE INFORMAZIONI

1. In conformità con le proprie leggi e regolamenti e procedure nazionali, entrambe le Parti Contraenti prenderanno le misure appropriate per proteggere le informazioni classificate, trasmesse, ricevute, generate o sviluppate in conseguenza di tale Accordo tra le Parti Contraenti. Le Parti Contraenti garantiranno a tutte le informazioni classificate scambiate, ricevute, originate o sviluppate lo stesso grado di protezione di sicurezza nella stessa misura fornita alle proprie informazioni classificate di equivalente livello, come specificato al successivo Articolo 6 del presente Accordo.

2. La Parte Contraente ricevente e/o i suoi enti non useranno un livello di classifica inferiore per informazioni classificate ricevute ne' declassificheranno tali informazioni senza la preventiva autorizzazione scritta della Parte Contraente originatrice. La Parte Contraente originatrice informerà la Parte Contraente che riceve in merito a qualsiasi cambiamento alle classifiche di sicurezza delle informazioni scambiate.

3. L'accesso alle informazioni classificate ed a siti e strutture in cui si effettuano attività classificate o dove sono custodite le informazioni classificate sarà limitato a coloro che siano provvisti di una abilitazione di sicurezza ed a chi, a causa della propria funzione o incarico, abbia "necessità di conoscere".

4. Ciascuna Parte Contraente sovrintenderà all'osservanza delle leggi, norme e procedure di sicurezza degli enti pubblici e/o privati che detengano, sviluppino, producano e/o usino informazioni classificate dell'altra Parte Contraente, a mezzo di, inter alia, visite ispettive.

5. Le Parti Contraenti non divulgheranno le informazioni classificate dell'altra Parte Contraente a Governi o Organizzazioni terze senza la previa autorizzazione della Parte Contraente che le ha fornite.

6. Il presente Accordo non potrà essere utilizzato dall'altra Parte Contraente per ottenere informazioni classificate che l'altra Parte Contraente abbia ricevuto da Governi Contraenti o Organizzazioni Terze.

ARTICOLO 4
ABILITAZIONE DI SICUREZZA

1. Ciascuna Parte Contraente garantirà che ogni soggetto, che a causa del suo impiego debba avere accesso ad informazioni classificate RISERVATISSIMO o di livello

superiore, sia in possesso di una valida ed adeguata abilitazione di sicurezz personale (NOS) emessa dall'Autorità Nazionale di Sicurezza o altra competente.

2. Le indagini personali tese a fornire una Abilitazione personale di Sicurezza, dovranno stabilire se la lealtà e l'affidabilità verso le leggi dello Stato della persona interessata possa consentire l'accesso ad informazioni classificate senza pericoli per la sicurezza.

3. Le Parti Contraenti, previa richiesta, in considerazione della rispettiva normativa interna, collaboreranno nella procedura di rilascio delle Abilitazioni personali d Sicurezza e delle Abilitazioni di Sicurezza societarie, concordate tra le rispettive Autorità Nazionali per la Sicurezza competenti.

ARTICOLO 5
RILASCIO DELLE INFORMAZIONI

1. Il rilascio delle informazioni classificate ricevute dall'altra Parte Contraente, a Stati terzi o Organizzazioni internazionali, in forza del presente Accordo, si effettuerà tramite i mezzi e le procedure concordate dalle Parti Contraenti originatrici, che potranno imporre ulteriori limitazione al rilascio.

2. Ciascuna Parte Contraente userà le informazioni classificate dell'altra Parte Contraente soltanto per lo scopo per cui tali informazioni sono rilasciate.

ARTICOLO 6
CLASSIFICHE DI SICUREZZA

1. Le classifiche di sicurezza applicabili alle informazioni scambiate di cui al presente Accordo e le loro equivalenze sono le seguenti

ESTONIA	ITALIA
TAIESTI SALAJANE	*SEGRETISSIMO*
SALAJANE	*SEGRETO*
KONFIDENTSIAALNE	*RISERVATISSIMO*

2. Le Parti Contraenti si impegneranno a proteggere le informazioni contrassegnate come di seguito, scambiate tra loro e/o enti pubblici e privati, in osservanza delle rispettive leggi e regolamenti:

AVALDAMISELE MITTEKUULUV ja/või AMETKONDLIK	*RISERVATO*

ARTICOLO 7
AUTORITA' COMPETENTI

1. Le competenti Autorità di Sicurezza responsabili per l'esecuzione ed i controlli attinenti a tutti gli aspetti del presente Accordo sono:

in Estonia:	in Italia
Office of National Security Coordinator *State Chancellery* *The Stenbock House* *Rahukohtu 3* *15161 Tallinn* *ESTONIA*	*Presidenza del Consiglio dei Ministri* *Autorità Nazionale per la Sicurezza* *CESIS – III Reparto U.C.Si.* *Via della Pineta Sacchetti, n.216* *00168 Roma* *ITALIA*

Ciascuna Parte Contraente si impegna ad assicurare che la rispettiva competente Autorità di Sicurezza osservi scrupolosamente i dettami del presente Accordo.

2. Ambedue le competenti Autorità di Sicurezza, ciascuna nella giurisdizione del proprio Stato, prepareranno, emaneranno e supervisioneranno le istruzioni e le procedure per la protezione delle informazioni classificate scambiate come risultato di ogni altro Accordo tra le Parti Contraenti.

3. Ciascuna delle Autorità di Sicurezza competenti, fornirà, su richiesta, alle altre competenti Autorità di Sicurezza le informazioni concernenti la propria organizzazione e le procedure di sicurezza al fine di raggiungere e mantenere gli stessi standard di sicurezza e facilitare visite congiunte in ambo i Paesi da parte di personale autorizzato. Ambo le Parti Contraenti si accorderanno circa le modalità di tale visite.

ARTICOLO 8
VISITE

1. Le visite a siti in cui si sviluppano, trattano o custodiscono informazioni classificate, o dove si eseguono progetti e/o contratti classificati saranno consentite da una Parte Contraente ai visitatori del Paese dell'altra Parte Contraente solo ove sia stato ottenuto un permesso scritto dalle competenti Autorità di Sicurezza della Parte Contraente ricevente. Tale permesso sarà accordato solamente a persone che siano state abilitate e che abbiano "necessità di conoscere".
2. Le procedure relative alle visite saranno definite e concordate tra le Competenti Autorità di Sicurezza indicate al precedente art.7.

3. Ciascuna Parte Contraente garantirà la protezione dei dati personali dei visitatori nell'osservanza delle leggi e regolamenti nazionali in vigore.

ARTICOLO 9
SICUREZZA INDUSTRIALE

1. Nel caso in cui ciascuna delle Parti Contraenti e/o le sue agenzie o enti interessati dagli argomenti di cui all'art. 1 risulti aggiudicataria di un contratto per prestazioni nel territorio dell'altra Parte Contraente, e tale contratto interessi informazioni classificate, la Parte Contraente del Paese ove sta avendo luogo la prestazione ai sensi dell'Accordo assumerà la responsabilità della trattazione di tali informazioni classificate nell'osservanza delle proprie esigenze e standard.

2. Prima del rilascio ai contraenti o possibili contraenti dell'altra Parte Contraente di qualsiasi informazione classificata ricevuta dall'altra Parte Contraente, la Parte Contraente ricevente dovrà:

   a. dare assicurazione che tali contraenti o possibili contraenti e relative ditte abbiano la capacità di proteggere adeguatamente informazioni classificate;
   b. concedere un'adeguata abilitazione di sicurezza societaria ai contraenti interessati;
   c. concedere un'adeguata abilitazione personale di sicurezza a tutto il personale che in ragione del suo impiego dovrà avere accesso ad informazioni classificate;
   d. assicurare che tutte le persone che avranno accesso alle informazioni classificate, vengano informate sulle loro responsabilità nella protezione delle informazioni classificate in applicazione delle leggi in vigore.

3. Ogni contratto classificato tra enti pubblici e/o privati delle Parti Contraenti includerà una specifica sezione di sicurezza ed una lista di classifiche di sicurezza basate sui termini del presente Accordo.
   La competente Autorità di Sicurezza, nel cui Paese si dovrà effettuare l'attività, assumerà la responsabilità per quanto riguarda la prescrizione e gestione delle misure di sicurezza del contratto con gli stessi standard ed esigenze che tutelano la protezione dei propri contratti classificati.
   L'elenco dei possibili sub-contraenti interessati in contratti classificati verrà preventivamente sottoposto dai contraenti alle competenti Autorità di Sicurezza per l'approvazione. In caso di buon fine, la lista dei possibili sub-contraenti dovrà soddisfare agli stessi obblighi di sicurezza stabiliti per il contraente.

4. La notifica di qualsiasi progetto, Accordo, contratto o sub-contratto classificato, verrà precedentemente notificato alle competenti Autorità di Sicurezza della Parte Contraente in cui il progetto dovrà realizzarsi.

Due -2- copie dell'appendice di sicurezza di ogni contratto classificato verranno inoltrate alla competente Autorità di Sicurezza nel cui Paese il lavoro o progetto dovrà essere realizzato.

5. Le Parti Contraenti proteggeranno i diritti d'autore, la proprietà dei diritti industriali, brevetti inclusi, ed ogni altro diritto connesso alle informazioni reciprocamente scambiate.

ARTICOLO 10
TRASFERIMENTO DELLE INFORMAZIONI CLASSIFICATE

1. Le informazioni classificate verranno normalmente trasmesse tra le Parti Contraenti attraverso i rispettivi canali diplomatici.
Lo scambio delle informazioni classificate potrà avvenire tramite rappresentanti ufficialmente accreditati dalle competenti Autorità di Sicurezza di ambedue le Parti Contraenti. Ogni autorizzazione può, ove richiesto, essere concessa ai rappresentanti di imprese industriali impegnati in specifici progetti.

2. Lo scambio di materiali di grandi dimensioni o di informazioni classificate in gran numero, verrà stabilita caso per caso dalle competenti Autorità di Sicurezza.

3. Altri mezzi di trasmissione e di scambio, approvati, potranno essere concordati tra le competenti Autorità di Sicurezza.

ARTICOLO 11
VIOLAZIONI DI SICUREZZA E COMPROMISSIONI

1. In caso di infrazione alla sicurezza da cui derivi la certezza o una sospetta compromissione di informazioni classificate, originate o ricevute dall'altra Parte Contraente, la competente Autorità di Sicurezza nel cui Paese la compromissione si è verificata, informerà la competente Autorità di Sicurezza dell'altra parte Contraente appena possibile e condurrà le adeguate indagini.
L'altra Parte Contraente, ove richiesta, collaborerà all'indagine.

2. In ogni caso, l'altra Parte Contraente dovrà essere informata sui risultati dell'indagine e riceverà il rapporto finale sui motivi dell'evento e la valutazione del danno.

ARTICOLO 12
SPESE

1. L'esecuzione del presente Accordo non comporterà di norma alcun costo.

2. In caso di eventuali costi, ciascuna delle Parti Contraenti li sopporterà in osservanza alle proprie leggi e regolamenti nazionali. In nessun caso i costi sostenuti da una Parte Contraente potranno essere imposti all'altra Parte Contraente.

ARTICOLO 13
CONTROVERSIE

1. Eventuali controversie riguardanti l'interpretazione o l'applicazione del presente Accordo verranno risolte amichevolmente previa consultazione delle Parti Contraenti.

ARTICOLO 14
VARIE

1. I titoli di ciascun articolo debbono intendersi esclusivamente come comodità di riferimento e non devono intendersi ne usarsi per altri scopi che ne possano in alcun modo limitare o estendere il linguaggio dei provvedimenti a cui il titolo si riferisce.

2. Le Parti Contraenti non avranno alcun diritto di assegnare o altrimenti trasferire i diritti o obblighi in forza del presente Accordo, senza il consenso scritto dell'altra Parte Contraente.

3. Ciascuna Parte Contraente assisterà il personale dell'altra Parte Contraente nell'esercizio dei servizi e/o diritti in conformità degli adempimenti del presente Accordo nel Paese della controparte.

4. In caso in cui si presentasse la necessità, le Autorità di Sicurezza delle Parti Contraenti, si consulteranno vicendevolmente sugli specifici aspetti tecnici concernenti l'adempimento del presente Accordo e potranno di comune accordo stabilire, di volta in volta, la stipula di protocolli di sicurezza supplèmentari al presente Accordo.

ARTICOLO 15
DISPOSIZIONI FINALI

1. Il presente Accordo avrà durata illimitata ed entrerà in vigore il primo giorno successivo alla data della ricezione della seconda delle due notifiche con cui le Parti Comtraenti si saranno comunicate ufficialmente l'avvenuto espletamento delle rispettive procedure interne all'uopo previste.

2. Ciascuna delle Parti Contraenti avrà il diritto di rescindere il presente Accordo. A tal fine, una comunicazione scritta di recesso sarà consegnata alla controparte almeno sei mesi prima.

3. Ciascuna delle Parti Contraenti notificherà prontamente alla controparte qualsiasi cambiamento delle proprie leggi e regolamenti che potrebbero incidere sulla protezione delle informazioni classificate di cui al presente Accordo. In tal caso, le Parti Contraenti si consulteranno per esaminare la possibilità di modifiche al presente Accordo. Al tempo stesso, le informazioni classificate continueranno ad essere protette, come previsto, salvo che diversamente stabilito per iscritto dalla Parte Contraente rilasciante.

4. Malgrado la rescissione del presente Accordo, tutte le informazioni classificate rilasciate in forza del presente Accordo, continueranno ad essere protette secondo quanto stabilito.
   Inoltre, speciali categorie di informazioni o materiali classificati scambievolmente concordati dalle competenti Autorità di Sicurezza delle Parti Contraenti e debitamente designati come tali, saranno restituiti, previa richiesta, alla Parte Contraente originatrice.

5. Revisioni, cambiamenti o emendamenti al presente Accordo, si possono effettuare in qualsiasi momento, previo consenso scritto di ambedue le Parti Contraenti.

6. In caso di cessazione, materiali e/o informazioni classificate ai termini del presente Accordo saranno restituiti alla controparte appena possibile. Materiali e/o informazioni classificate che non siano restituiti saranno protetti in osservanza dei provvedimenti stabiliti nel presente Accordo.

In fede di che i sottoscritti Rappresentanti, debitamente autorizzati dai rispettivi Governi, hanno firmato il presente Accordo.
Fatto a Tallinn il 23. 11. 2000 in lingua estone ed italiana, essendo ambedue i testi ugualmente validi.

Per il Governo della Repubblica di Estonia

Per il Governo della Repubblica Italiana

[TRANSLATION - TRADUCTION]

AGREEMENT BETWEEN THE GOVERNMENT OF THE REPUBLIC OF ESTONIA AND THE GOVERNMENT OF THE ITALIAN REPUBLIC FOR THE MUTUAL PROTECTION OF CLASSIFIED INFORMATION

I. The Government of the Republic of Estonia and the Government of the Italian Republic, hereinafter referred to as the Contracting Parties, wishing to guarantee the mutual protection of all classified information which is exchanged directly or through other public agencies or private organizations under the jurisdiction of the Contracting Parties, is included in government documents or is covered by government agreements, have agreed as follows:

Article 1. Scope

I. This Agreement shall apply to activities of any kind involving the exchange of classified information between the Contracting Parties in respect of the following:

(a) Cooperation between the Contracting Parties relating to national defence or any other matter involving national security;

(b) Cooperation, joint ventures, contracts and all other arrangements between public and private entities of the Contracting Parties relating to national defence or any other matter involving national security;

(c) Sale by one Contracting Party to the other of equipment or technical expertise relating to defence or national security.

Article 2. Definitions

1. For the purposes of this Agreement:

The term "classified information" means:

(a) Any document or material referred to in subparagraphs (b) and (c) below or any transaction, information, activity and the like which has been so designated by security classification;

(b) The term "classified document" means any classified information regardless of its physical form or characteristics, including, without limitation, written or printed information, data-processing cards and tapes, maps, photographs, pictures, drawings, engravings, sketches, working notes, carbon copies and ink ribbons or reproductions by any means or process, and sound, voice, magnetic or electronic or optical or video recordings in any form, and portable automated data processing (ADP) equipment with resident or removable computer storage media;

(c) The term "classified material" means any object or item of machinery, prototype, equipment, weapon, etc., either produced or in the process of being produced by machine or by hand, which has been assigned a security classification;

(d) The term "security classification" means one of the classifications specified in article 6 below.

The term "classified contract" means an agreement between two or more Contracting Parties establishing the reciprocal rights and duties of the parties, which contains or provides for the use of classified information;

The term "contractor or subcontractor" means a natural or legal person with the legal capacity to enter into contracts;

The term "breach of security" means an act or omission contrary to national security standards which has consequences that might jeopardize or compromise classified information;

The term "compromise of security" means the actual transmission, in whole or in part, of knowledge of classified information to persons or entities or States not possessed of the proper security clearance or authorized access to such knowledge, or the possibility that such transmission could have occurred;

The term "personal security clearance" means a favourable determination as a result of a screening procedure designed to determine the loyalty and trustworthiness of an individual, on the basis of which that person may have access to and handle classified information up to a given classification level in accordance with the applicable national security rules;

The term "facility security clearance" means a favourable determination as a result of a screening procedure designed to determine the physical and organizational capability of a public and/or private entity to handle a certain level of classified information, in accordance with applicable national security laws and regulations;

The term "need to know" means the principle according to which access to classified information may be granted only to persons who objectively need the information for the performance of their official duties, for which purpose the information has been released to the Contracting Party receiving it.

Article 3. Protection of information

1. The two Contracting Parties shall, in accordance with their own national laws, regulations and procedures, take appropriate measures to protect classified information transmitted, received, generated or developed pursuant to an agreement to that effect between them. The Contracting Parties shall ensure that all classified information exchanged, received, originated or developed is afforded the same degree of security protection as is afforded to their own classified information of the corresponding classification level, as specified in article 6 below.

2. The receiving Contracting Party and/or its agencies shall not downgrade the classification level of any classified information received or declassify such information without the prior written consent of the originating Contracting Party. The originating Contracting Party shall inform the receiving Contracting Party of any change in the security classification of the information exchanged.

3. Access to classified information and to areas and facilities in which classified activities are conducted or where classified information is stored shall be restricted to persons

who have security clearance and who, because of their specific duties or office, have a "need to know".

4. Each Contracting Party shall supervise the observance of security laws, standards and procedures by public and/or private entities which hold, develop, produce and/or use classified information of the other Contracting Party, by means of, inter alia, inspection visits.

5. Neither of the Contracting Parties shall disclose the classified information of the other Party to third-country Governments or organizations without the prior consent of the Party providing the information.

6. This Agreement may not be used by one Contracting Party to obtain any classified information received by the other Contracting Party from contracting Governments or third-country organizations.

Article 4. Security clearance

1. Each Contracting Party shall ensure that all persons who, in the conduct of their official duties, require access to information classified CONFIDENTIAL and above have valid and appropriate security clearance issued by the national security authorities or another competent body.

2. The individual screening required for personal security clearance must establish if the loyalty and trustworthiness of the person concerned are such as to warrant access to classified information without any risk to security.

3. Upon request, the Contracting Parties, taking into account their respective domestic laws and regulations, shall cooperate in carrying out the personal security clearance and facility security clearance procedures agreed to by their respective national security authorities competent in the matter.

Article 5. Release of information

1. Classified information received from the other Contracting Party pursuant to this Agreement shall be released to third countries or to international organizations in accordance with the practices and procedures stipulated by the originating Party, which may impose restrictions on the release.

2. Each Contracting Party shall use the classified information of the other Contracting Party solely for the purpose for which the information was provided.

Article 6. Security classifications

1. The equivalent security classifications applicable to information exchanged under the terms of this Agreement are as follows:

Estonia

Estonia	*In Italie*
TEIESTI SALAJANE	SEGRETISSIMO
TAIESTI SALAJANE	SEGRETISSIMO
SALAJANE	SEGRETO
KONFIDENTSIAALNE	RISERVATISSIMO

2. In accordance with their respective laws and regulations, the Contracting Parties undertake to protect information which they have exchanged with one another and/or with public or private entities and which has been designated as follows:

AVALDAMISELE	RISERVATO
MITTEKUULUV ja/vòi	
AMETKONDLIK	

Article 7

Competent authorities

1. The security authorities responsible for the implementation and the relevant monitoring of all aspects of this Agreement shall be:

IN Estonia:	*In Italia*
Office of National Security coordinator	Presidenza del Consiglio dei Ministri
State Chancellery	Autorità Nazionale per la Sicurezza
The Stenbock House	CESIS - III REparto U.C.Si.
Rahukohtu 3	Via della Pineta Sacchetti, n.216
15161 Tallinn	00168 Roma
ESTONIA	ITALIA

Each Contracting Party undertakes to ensure that its competent security authorities scrupulously observe the requirements of this Agreement.

2. The two competent security authorities, within the jurisdiction of their respective States, shall prepare, issue and supervise instructions and procedures for the protection of classified information exchanged as a result of any other agreement between the Contracting Parties.

3. Upon request, each of the competent security authorities shall provide information to the other competent security authorities concerning their own organization and security procedures with a view to meeting and maintaining the same security standards and facilitating joint visits in the two countries by authorized personnel. The two Contracting Parties shall agree on the arrangements for such visits.

Article 8. Visits

1. Visits to areas where classified information is developed, handled or stored or where classified projects and/or contracts are carried out shall be permitted by one Contracting Party in the case of visitors from the country of the other Contracting Party only after written authorization has been obtained from the competent security authorities of the receiving Contracting Party. Such written authorization shall be granted only to persons who have been security screened and who have a "need to know".

2. The procedures relating to visits shall be established by agreement between the national security authorities referred to in article 7 above.

3. Each Contracting Party shall ensure that the personal data of visitors are protected in accordance with the national laws and regulations in force.

Article 9. Industrial security

1. Where either Contracting Party and/or any of its agencies or entities to which the provisions of article 1 apply awards a contract for services in the territory of the other Contracting Party and that contract involves classified information, the Contracting Party in whose country services covered by this Agreement are being performed shall assume responsibility for handling such classified information in accordance with its own requirements and standards.

2. Before a Contracting Party releases to its contractors or prospcctive contractors any classified information received from the other Contracting Party, the receiving Contracting Party shall:

(a) Provide assurances that such contractors or prospective contractors and their corresponding enterprises have the capability to protect classified information adequately;

(b) Grant appropriate facility security clearance to the contractors concerned;

(c) Grant appropriate personal security clearance to all personnel who by reason of their official duties will need to have access to classified information;

(d) Ensure that all persons who will have access to classified information are informed of their responsibility to protect the classified information under the laws in force.

3. Every classified contract between public and/or private entities of the Contracting Parties shall include a separate section on security and a list of security classifications based on the terms set out in this Agreement.

The competent security authorities in whose country the activity is to be conducted shall assume responsibility for prescribing and overseeing the security measures stipulated in the contract, observing the same standards and requirements as govern the protection of that country's own classified contracts.

A list of the prospective subcontractors involved in a classified contract shall be submitted in advance by the contractor to the competent security authorities for approval. If approved, the prospective subcontractors on the list shall satisfy the same security requirements as those established for the contractor.

4. Prior notification of each classified project, agreement, contract or subcontract shall be given to the competent security authorities of the Contracting Party in whose country the work is to be carried out.

Two copies of the security annex to every classified contract shall be forwarded to the competent security authorities in whose country the work or project is to be carried out.

5. The Contracting Parties shall protect copyrights, ownership of industrial rights, including patents, and any other rights associated with the information exchanged between them.

Article 10. Transfer of classified information

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

The exchange of classified information may be made through representatives officially accredited by the competent security authorities of the two Contracting Parties. Full authorization may upon request be granted to representatives of industrial enterprises who are engaged in specific projects.

2. The exchange of very bulky material or of large quantities of classified information shall be determined in each individual case by the competent security authorities.

3. Other approved means of transmission and exchange may be mutually agreed by the competent security authorities.

Article 11. Breach or compromise of security

1. In the case of a breach of security resulting in a known or suspected compromise of classified information originated by or received from the other Contracting Party, the competent security authorities in whose country the compromise proves to have occurred shall inform the competent security authorities of that other Contracting Party without delay and shall conduct an appropriate investigation.

The other Contracting Party shall upon request take part in the investigation.

2. The other Contracting Party shall in all cases be informed of the outcome of the investigation and shall receive the final report giving the reasons for the occurrence and an assessment of the damage.

Article 12. Costs

1. The implementation of this Agreement will not as a rule entail any costs.

2. Should there be any costs, each Contracting Party shall defray them in accordance with its own national laws and regulations. In no case may the costs incurred by one Contracting Party be imposed on the other Contracting Party.

Article 13. Disputes

1. Any disputes arising from the interpretation or implementation of this Agreement shall be resolved amicably after consultation between the Contracting Parties.

Article 14. Miscellaneous

1. All the above titles of articles are to be understood solely as having been included for ease of reference and shall not be interpreted or used for other purposes which might in any way restrict or broaden the language of the provisions to which the titles refer.

2. Neither Contracting Party shall have any right to assign or otherwise transfer the rights and obligations arising from this Agreement without the written consent of the other Contracting Party.

3. Each Contracting Party shall assist the personnel of the other Contracting Party in the exercise of functions and/or rights in connection with the implementation of this Agreement in the counterpart country.

4. Where necessary, the security authorities of the Contracting Parties shall consult each other on specific technical points involved in the implementation of this Agreement and may from time to time decide by mutual agreement to conclude security protocols supplementary to this Agreement.

Article 15. Final provisions

1. This Agreement shall remain in force indefinitely and shall enter into force on the first day following the date of receipt of the second of the two notifications by which the Contracting Parties officially inform each other that their respective internal procedures for its entry into force have been completed.

2. Each Contracting Party shall have the right to terminate this Agreement. To that end, the other Party shall be given notice of termination in writing at least six months in advance.

3. Each Contracting Party shall promptly notify the other of any changes to its own laws and regulations which might have an effect on the protection of the classified information referred to in this Agreement. In such a case, the Contracting Parties shall consult

with one another to discuss the possibility of amending this Agreement. In the meantime, the classified information shall continue to be protected as provided, unless otherwise established in writing by the Contracting Party which released it.

4. Notwithstanding the termination of this Agreement, all classified information released pursuant to this Agreement shall continue to be protected in accordance with the provisions set forth herein.

Moreover, special categories of classified information or material duly designated as such by the mutual agreement of the competent security authorities of the Contracting Parties shall upon request be returned to the originating Contracting Party.

5. This Agreement may be reviewed, modified or amended at any time by the mutual agreement of the Contracting Parties in writing.

6. In the event of termination, classified material and/or information under this Agreement shall be returned to the other Party without delay. Classified material and/or information which is not returned shall be protected in accordance with the provisions of this Agreement.

In witness whereof, the undersigned representatives, being duly authorized thereto by their respective Governments, have signed this Agreement.

Done at Tallinn on 23 November 2000, in the Estonian and Italian languages, both texts being equally authentic.

For the Government of the Republic of Estonia:

[ERIK-NIILES KROSS]

For the Government of the Italian Republic:

[FERNANDO MASONE]

[TRANSLATION -- TRADUCTION]

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

1. Le Gouvernement de la République d'Estonie et le Gouvernement de la République italienne, ci-après dénommés les Parties contractantes, souhaitant garantir la protection mutuelle de toutes les informations classifiées, échangées directement ou par l'intermédiaire d'organismes publics ou d'organisations privées relevant de la juridiction des Parties contractantes, et figurant dans les documents officiels ou couverts par des accords gouvernementaux, sont convenus de ce qui suit :

Article premier. Portée

1. Le présent Accord s'applique aux activités de toutes sortes concernant l'échange d'informations classifiées entre les Parties contractantes dans les domaines suivants :

a) Coopération entre les Parties contractantes liée à la défense nationale ou à toute autre question intéressant la sécurité nationale ;

b) Coopération, co-entreprises, contrats et tous autres accords entre des entités publiques et privées des Parties contractantes, liés à la défense nationale ou à toute autre matière mettant en jeu la sécurité nationale;

c) Vente par une Partie contractante à l'autre de matériel ou d'expertise techniques intéressant la défense ou la sécurité nationale.

Article 2. Définitions

1. Aux fins du présent Accord :

L'expression "information classifiée" s'entend de:

a) Tout document ou matière mentionnés aux alinéas b) et c) ci-dessous ou de toute transaction, information, activité et autre, ainsi désignées par la classification relative à la sécurité;

b) L'expression "document classifié" s'applique à toutes les informations classifiées quelles que soient leur présentation physique ou leurs caractéristiques, y compris mais non exclusivement, des renseignements écrits ou imprimés, des cartes informatiques et des bandes magnétiques, des cartes, des photographies, des tableaux, des dessins, des gravures, des esquisses, des notes de travail, des copies de carbone et des rubans encrés ou des reproductions obtenues par n'importe quels moyens ou procédés, et des enregistrements sonores, vocaux, magnétiques ou électroniques ou optiques ou vidéos, sous quelque forme que ce soit, ainsi que des équipements portables de données automatisées (ADP) accompagnés de stockage fixe ou mobile des données électroniques;

c) L'expression "matière classifiée" s'entend de tout objet ou article de machine, prototype, équipement, arme, réalisé ou en cours de production, mécaniquement ou manuellement, auquel a été attribué une classification dans le domaine de la sécurité ;

d) L'expression "classification de sécurité" s'entend d'une des classifications quelconques spécifiées à l'article 6 ci-dessous.

L'expression "contrat classifié" désigne tout accord entre deux ou plusieurs Parties contractantes, déterminant les droits et les obligations réciproques des parties, qui contient ou prévoit des dispositions pour l'utilisation d'informations classifiées.

Les termes "contractant ou sous-traitant" s'entendent d'une personne physique ou morale ayant la capacité légale ou juridique de signer des contrats;

L'expression "manquement à la sécurité" s'entend d'un acte ou d'une omission contraire aux normes de sécurité nationale et qui a des conséquences susceptibles de compromettre ou de détruire des informations classifiées;

L'expression "compromission sur la sécurité" s'entend de la transmission effective, totale ou partielle, de connaissances sur des informations classifiées à des personnes ou des entités ou des États qui ne disposent pas des moyens satisfaisants au point de vue sécurité ou n'ont pas l'autorisation d'accéder a' ces connaissances ou la possibilité de procéder à ce type de transmission.

L'expression "habilitation personnelle de sécurité" s'entend d'une décision favorable à la suite d'une procédure de vérification visant à s'assurer de la loyauté d'un individu et de la confiance qu'on peut lui accorder, sur la base de laquelle ladite personne peut obtenir ou traiter des informations classifiées jusqu'à un niveau de classification déterminé, conformément aux règles nationales applicables en matière de sécurité.

L'expression "habilitation des dispositifs de sécurité" signifie une décision favorable à la suite d'un contrôle visant à déterminer la capacité physique et organisationnelle d'un organisme public et/ou privé à traiter des informations classifiées d'un niveau déterminé, conformément aux lois et réglementations nationales en matière de sécurité.

L'expression "besoin de savoir" s'applique au principe suivant lequel l'accès à des informations classifiées ne peut être accordé qu'à des personnes qui objectivement ont besoin des informations, qui ont été communiquées à la Partie contractante qui les reçoit, pour accomplir leurs fonctions officielles.

Article 3. Protection de l'information

1. Les deux Parties contractantes, conformément à leurs législations, réglementations et procédure nationales, prennent les mesures appropriées pour protéger les informations classifiées, transmises, reçues, produites ou élaborées, conformément à un accord passé entre elles à cette fin. Elles s'assurent que toutes les informations classifiées, échangées, reçues, produites ou élaborées bénéficient du même degré de protection en matière de sécurité que celui dont elles jouissent dans leur propre classification, comme spécifié à l'article 6 ci-dessous.

2. La Partie contractante qui reçoit l'information et/ou ses organismes ne doivent pas abaisser le niveau de classification des informations classifiées reçues, ou déclassifier ces

informations, sans informer la Partie contractante réceptrice de toute modification dans la classification de la sécurité des informations échangées.

3. L'accès aux informations classifiées et aux secteurs et installations dans lesquels les activités classifiées sont entreprises ou les informations classifiées emmagasinées est limité aux personnes qui ont une habilitation en matière de sécurité et qui, du fait de leurs attributions spécifiques, ont "besoin de savoir".

4. Chaque Partie contractante surveille l'application des lois, normes et procédures en matière de sécurité par les organismes publics et/ou privés qui détiennent, élaborent, produisent et/ou utilisent les informations classifiées de l'autre Partie contractante, grâce notamment à des visites d'inspection.

5. Aucune des Parties contractantes ne communique les informations classifiées de l'autre Partie contractante à des Gouvernements ou organisations tiers sans avoir obtenu au préalable le consentement de la Partie qui a fourni l'information.

6. Le présent Accord ne peut être utilisé par une Partie contractante pour obtenir des informations classifiées reçues par l'autre Partie contractante en provenance de Gouvernements ou d'organisations nationales de pays tiers.

Article 4. Habilitations de sécurité

1. Chaque Partie contractante veille à ce que toutes les personnes qui, dans l'exercice de leurs fonctions officielles, ont besoin de l'accès aux informations classifiées CONFIDENTIEL et au-dessus, disposent d'une habilitation valide et adéquate de sécurité, émise par les autorités chargées d'assurer la sécurité nationale ou par un autre organisme compétent.

2. La personne chargée d'examiner les demandes d'habilitation personnelle de sécurité doit juger si la loyauté de la personne concernée et la confiance qu'on peut lui accorder sont suffisantes pour justifier un accès aux informations classifiées sans risque pour la sécurité.

3. Sur demande, les Parties contractantes ayant pris en compte leurs législations et réglementations nationales coopèrent dans l'exécution des procédures concernant les habilitations personnelles et celles concernant les moyens liés à la sécurité, acceptées par leurs autorités nationales respectives compétentes.

Article 5. Communication de l'information

1. Les informations classifiées reçues de l'autre Partie contractante conformément au présent Accord sont communiquées à des pays tiers ou à des organisations internationales conformément aux pratiques et procédures stipulées par la Partie d'où elles proviennent et qui peut imposer des restrictions quant à leur communication.

2. Chaque Partie contractante utilise les informations classifiées de l'autre Partie contractante uniquement pour l'objectif pour lequel l'information a été fournie.

Article 6. Classifications en matière de sécurité

1. Les équivalences en matière de classification dans le domaine de la sécurité, applicables aux informations échangées au titre du présent Accord s'établissent comme suit :

ESTONIE		*ITALIE*
SECRET D'ETAT	TAIESTI SALA	SEGRETISSIMO
SECRET	SALAJANE	SEGRETO
CONFIDENTIEL	KONFIDENTSIAANE	RISERVATISSIMO

2. Conformément à leurs législations et réglementations respectives, les Parties contractantes s'engagent à protéger les informations qu'elles ont échangées entre elles ou avec des entités publiques ou privées et qui ont été désignées comme suit :

ESTONIE		*ITALIE*
RESTREINT	AVALDAMIESELE MITTEK-UULUV	RISERVATO
ET/OU UTILISATION		
OFFICIELLE		
SEULEMENT	ET/OU AMETKOND-LIK	

Article 7. Autorités compétentes

1. Les autorités chargées de la sécurité pour l'application et le suivi de tous les aspects du présent Accord sont:

ESTONIE	*ITALIE*
Cabinet du coordinateur en matière de sécurité nationale	Cabinet du Président du Conseil des Ministres
Chancellerie	Direction de la Sécurité nationale

ESTONIE	*ITALIE*
The Stenbock House	Comité exécutif des Services pour l'information et la Sécurité (CESIS)
Rahukohtu 3	Département III, service central de Sécurité
15161 Tallinn	Via della Pineta Sacchetti, 00168
Estonie	Rome Italie

Chaque Partie contractante s'engage à veiller à ce que ses autorités compétentes respectent scrupuleusement les obligations du présent Accord.

2. Les deux autorités compétentes, selon la juridiction de leurs États respectifs, établissent, publient et surveillent les instructions et les procédures visant à assurer la protection des informations classifiées, échangées du fait d'un autre accord entre les Parties contractantes.

3. Sur demande, chacune des autorités compétentes en matière de sécurité fournit des informations à l'autre autorité compétente sur sa propre organisation et ses procédures en matière de sécurité en vue d'obtenir et de maintenir le même niveau de normes de sécurité et de faciliter les visites communes dans les deux pays par le personnel habilité. Les deux Parties contractantes conviennent des dispositions concernant ces visites.

Article 8. Visites

1. Les visites dans les secteurs où les informations classifiées sont élaborées, traitées ou stockées ou dans ceux où les projets ou les contrats classifiés sont exécutés, sont autorisées par une Partie contractante dans le cas de visiteurs du pays de l'autre Partie contractante uniquement sur autorisation écrite accordée par les autorités compétentes de la Partie contractante qui reçoit la visite. Cette autorisation écrite n'est accordée qu'aux personnes qui ont été sélectionnées et qui ont "besoin de savoir".

2. Les procédures concernant les visites sont fixées par accord entre les autorités nationales compétentes mentionnées dans l'article 7 ci-dessus.

3. Chaque Partie contractante veille à ce que les données personnelles des visiteurs soient protégées conformément à la législation et à la réglementation nationales en vigueur.

Article 9. Sécurité industrielle

1. Lorsque l'une ou l'autre des Parties contractantes ou l'une de ses organisations ou entités, auxquelles s'appliquent les dispositions de l'article premier, attribue un contrat pour des services sur le territoire de l'autre Partie contractante et que le contrat en question met en jeu des informations classifiées, la Partie contractante sur le territoire de laquelle les ser-

vices faisant l'objet de l'accord en question doivent être fournis est chargée du traitement de ces informations classifiées, conformément à ses propres normes et prescriptions.

2. Avant qu'une Partie contractante communique à ces entrepreneurs ou futurs entrepreneurs toute information envoyée par l'autre Partie contractante, la Partie contractante qui les reçoit :

a) Donne les assurances nécessaires que lesdits entrepreneurs ou futurs entrepreneurs et leur entreprise sont capables de protéger adéquatement les informations classifiées;

b) Accorde les autorisations adéquates en matière de sécurité des installations aux entrepreneurs intéressés,

c) Accorde les habilitations personnelles adéquates à toutes les personnes qui, du fait de leurs fonctions officielles, auront besoin d'accéder aux informations classifiées,

d) Veille à ce que toutes les personnes qui ont accès aux informations classifiées soient informées de leurs responsabilités en matière de protection des informations classifiées aux termes de la législation en vigueur.

3. Chaque contrat classifié signé entre entités publiques et/ou privées des Parties contractantes contient une section distincte sur la sécurité et une liste des classifications de sécurité, basées sur les conditions énumérées dans le présent Accord.

Les autorités compétentes en matière de sécurité, dans le pays desquelles l'activité doit être entreprise, se chargent de définir les mesures en matière de sécurité stipulées dans le contrat, d'en assurer le respect et d'adopter les mêmes normes et exigences que celles qui régissent la protection de leurs propres contrats classifiés.

Une liste des sous-traitants possibles figurant dans un contrat classifié est soumise au préalable par l'entrepreneur aux autorités compétentes pour approbation. S'ils sont acceptés, les futurs sous-traitants figurant sur la liste doivent satisfaire aux mêmes exigences en matière de sécurité que celles qui sont établies pour l'entrepreneur.

4. La notification préalable de chaque projet classifié, contrat ou accord de sous-traitance est faite aux autorités compétentes de la Partie contractante dans le pays desquelles les travaux ou le projet doivent être entrepris.

Deux exemplaires d'une annexe sur la sécurité pour chaque contrat classifié sont transmis aux autorités compétentes du pays dans lequel les travaux ou les projets doivent être exécutés.

5. Les Parties contractantes protègent les brevets, les droits d'auteur, la propriété des droits industriels, y compris les brevets et autres droits associés aux informations échangées entre elles.

Article 10. Transfert des informations classifiées

1. Les informations classifiées sont normalement transmises entre les Parties contractantes par la voie diplomatique.

L'échange d'informations classifiées peut avoir lieu par l'intermédiaire de représentants officiellement accrédités par les autorités compétentes des deux Parties contractantes.

Une autorisation totale peut sur demande être accordée aux représentants des entreprises industrielles chargées de projets spécifiques.

2. L'échange de matériel très volumineux ou de grandes quantités d'informations classifiées est mis au point dans chaque cas par les autorités compétentes.

3. D'autres moyens de transmission et d'échange approuvés peuvent être convenus entre les autorités compétentes.

Article 11. Violation de la sécurité ou compromission à ce sujet

1. Dans le cas de violation de la sécurité entraînant une compromission connue ou soupçonnée au sujet d'informations classifiées produite par l'autre Partie contractante ou reçue par elle, les autorités compétentes du pays dans lequel la compromission a été constatée informent les autorités compétentes de cette autre Partie contractante sans retard et mènent une enquête appropriée.

L'autre Partie contractante participe sur demande à l'enquête.

2. L'autre Partie contractante est dans tous les cas informée du résultat de l'enquête et reçoit le rapport définitif donnant les raisons de l'incident et une évaluation des dommages.

Article 12. Coûts

1. En principe, l'application du présent Accord n'entraînera pas de dépenses.

2. Cependant, si tel était le cas, chaque Partie contractante les assumera conformément à sa propre législation et réglementation nationale. Les dépenses engagées par une Partie contractante ne peuvent en aucun cas être imposées à l'autre Partie contractante.

Article 13. Différends

1. Tout différend résultant de l'interprétation ou de l'application du présent Accord est résolu à l'amiable après consultation entre les Parties contractantes.

Article 14. Dispositions diverses

1. Tous les titres des articles ci-dessus doivent être interprétés comme ayant été inclus uniquement pour faciliter les références et ne doivent pas être interprétés ou utilisés à d'autres fins qui pourraient d'une façon quelconque restreindre ou élargir le libellé des dispositions auxquelles se rapportent les titres.

2. Aucune des Parties contractantes n'a le droit de fixer ou de transférer des droits ou des obligations résultant du présent Accord sans le consentement écrit de l'autre Partie contractante.

3. Chaque Partie contractante aide le personnel de l'autre Partie contractante dans l'exercice de ses fonctions et/ou de ses droits, liés à l'application du présent Accord dans l'autre pays.

4. Le cas échéant, les autorités chargées de la sécurité des Parties contractantes se consultent sur des points techniques spécifiques soulevés par l'application du présent Accord et peuvent de temps à autre décider d'un commun accord de conclure des protocoles de sécurité pour compléter le présent Accord.

Article 15. Dispositions finales

1. Le présent Accord demeure en vigueur indéfiniment et prend effet le premier jour qui suit la date à laquelle est reçue la seconde des deux notifications, par lesquelles les deux Parties contractantes s'informent officiellement que leurs formalités internes respectives pour l'entrée en vigueur sont terminées.

2. Chaque Partie contractante a le droit de mettre fin au présent Accord. Dans ce cas, l'autre Partie reçoit une notification de dénonciation écrite, au moins six mois avant.

3. Chaque Partie contractante informe rapidement l'autre de tout changement apporté à sa propre législation et à ses réglementations susceptibles d'exercer une influence sur la protection des informations classifiées, mentionnées dans le présent Accord. Dans ce cas, les Parties contractantes se consultent pour examiner la possibilité de modifier le présent Accord. Entre temps, les informations classifiées continuent d'être protégées comme prévu, à moins d'une décision écrite différente prise par la Partie contractante qui l'a communiquée.

4. Nonobstant la dénonciation du présent Accord, toutes les informations classifiées communiquées conformément au présent Accord continuent d'être protégées selon les dispositions exposées plus haut.

En outre, des catégories spéciales d'informations classifiées ou de matériel dûment désigné comme tel d'un commun accord par les autorités compétentes des Parties contractantes sont, sur demande, renvoyées à la Partie contractante qui les a fournies.

5. Le présent Accord peut faire l'objet d'une révision, de modifications ou d'amendements en tout temps, après accord mutuel écrit des Parties contractantes.

6. En cas de dénonciation, le matériel et ou les informations classifiées au titre du présent Accord sont renvoyés à l'autre Partie sans retard. Lesdits matériel et/ou informations qui ne sont pas renvoyés sont protégés conformément aux dispositions du présent Accord.

En foi de quoi, les représentants soussignés, à ce dûment autorisés par leurs Gouvernements respectifs, ont signé le présent Accord.

Fait à Tallinn le 23 novembre 2000, en langues estonienne et italienne, les deux textes faisant également foi.

Pour le Gouvernement de la République d'Estonie :

[ERIK-NIILES KROSS]

Pour le Gouvernement de la République italienne :

[FERNANDO MASONE]