No. 38356

Estonia and Sweden

General Security Agreement between the Repuhlic of Estonia and the Kingdom of Sweden concerning the protection of classified information. Tallinn, 30 January 2002

Entry into force: *30 January 2002 by signature, in accordance with article 16*

Authentic texts: *English, Estonian and Swedish*

Registration with the Secretariat of the United Nations: *Estonia, 11 April 2002*

Estonie et Suède

Accord général de sécurité entre la République d'Estonie et le Royaume de Suède relatif à la protection des informations classifiées. Talliun, 30 janvier 2002

Entrée en vigueur : *30 janvier 2002 par signature, conformément à l'article 16*

Textes authentiques : *anglais, estonien et suédois*

Enregistrement auprès du Secrétariat des Nations Unies : *Estonie, 11 avril 2002*

[ENGLISH TEXT — TEXTE ANGLAIS]

GENERAL SECURITY AGREEMENT BETWEEN THE REPUBLIC OF ESTONIA AND THE KINGDOM OF SWEDEN CONCERNING THE PROTECTION OF CLASSIFIED INFORMATION

List of Contents

Introduction

The Republic of Estonia and the Kingdom of Sweden, also referred to as the Parties, have in the interest of national security, established the following General Security Agreement, wishing to ensure the protection of Classified Information transferred between the two countries for the purposes of defence research, production and procurement or to commercial and industrial organisations in both countries, through approved channels.

This Agreement is to be interpreted in accordance with national law.

Article 1. Definitions

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 mes-

sage, 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.

"Contract" means an agreement between two or more parties creating and defining enforceable rights and obligations between the Parties.

"Classified Contract" means a contract which contains or involves Classified Information.

"National Security Authority (NSA) / Designated Security Authority (DSA)" means the Government Authority responsible for Defence Security in each country.

"Originating Party" means the Party initiating the Classified Information as represented by the NSA / DSA.

"Recipient Party" means the Party to which the Classified Information is transmitted or transferred as represented by the NSA / DSA.

"Security Classifications" and their equivalents in the two countries are:

In Estonia	In Sweden
TÄIESTI SALAJANE	KVALIFICERAT HEMLIG
SALAJANE	HEMLIG
KONFIDENTSIAALNE	HEMLIG

Swedish classified information to be transmitted or transferred to the Republic of Estonia will, where possible, be marked both with the Swedish security classification and the corresponding Estonian classification.

On occasion either Party may ask the other to afford protection at a higher level but not at a lower level than the classification indicated.

Article 2. Competent Security Authorities

The Government Authorities responsible for Defence Security in each country are the following:

FOR SWEDEN

The NSA in Sweden responsible for Defence Security issues is:

Försvarsmakten

(The Swedish Armed Forces)

Headquarters

Military Intelligence and Security (MUST)

SE- 107 86 STOCKHOLM

Sweden

Phone no: +46 8 788 7500

Fax no: +46 8 788 8263

The DSA in Sweden responsible for Dcfence Security associated with defence materiel is:

Försvarets Materielverk

(The Swedish Defence Material Administration)

Security

SE- 115 88 STOCKHOLM

Sweden

Phone no: +46 8 782 4000

Fax no: +46 8 660 2251

FOR ESTONIA

The NSA in Estonia responsible for Defence Security associated with Defence Security issues is:

Security Department

Ministry of Defenee

Sakala 1, 15094

Tallinn, ESTONIA

Phone No: +372 6406 030

Fax No: + 172 6406 002

Article 3. Restrictions on Use and Disclosure

(1) Without prior consultation, recipients will not disclose or use, or permit the disclosure or use of, any Classified Information except for purposes and within the limitations stated by or on behalf of the Originating Party.

(2) The Recipient Party will not pass or disclose to a Government official, Contractor, Contractors employee or to any other person holding the nationality of any third country, or to any international organisation, any Classified Information, exchanged under the provisions of this Agreement, nor will it publicly disclose any Classified Information without the prior consultation of the Originating Party.

(3)) Nothing in this Agreement will be taken as an authority for, or govern the release, use, exchange or disclosure of intellectual property rights until the specific written authorisation of the owner of these rights has first been obtained, whether the owner is one of the Parties or a third party.

Article 4. Protection of Classified Information

(1) The Originating Party will ensure that the Recipient Party is informed of:

(a) the classification of the information and of any additional conditions of release or limitations on its use, and that documents are so marked; and

(b) any subsequent change in classification.

(2) The Recipient Party will:

(a) in accordance with its national laws and regulations, afford the equivalent level of security protection to Classified Information as is afforded by the Originating Party. The Receiving Party will take all steps legally available to it to keep transmitted and transferred Classified Information free from disclosure under any legislative provision, and each Party will maintain accountability and control procedures to manage the dissemination of, and access to, Classified Information.

(b) ensure that Classified Information is marked in accordance with Article I; and

(c) ensure that the classification is not altered, except as authorised in writing by or on behalf of the Originating Party .

(3) In order to achieve and maintain comparable standards of security, each NSA/DSA will, on request, provide to the other information about its security standards, procedures and practices for safeguarding Classified Information, and will for this purpose facilitate visits by the Competent Security Authorities.

Article 5. Access to Classified Information

Access to Classified Information will be limited to those persons who have a "need to know" and who have been security cleared by the recipient NSA / DSA, in accordance with their national standards, to the level appropriate to the classification of the information to be accessed.

Article 6. Transmission of Classified Information

(I) Classified Information will be transmitted between the two countries in accordance with the national security regulations of the Originating Party. One route will be through official diplomatic Government to Government channels, but other Arrangements may be established, such as hand carriage, secure communications (encryption), if mutually acceptable to both Parties. The Party receiving Classified Information shall acknowledge its receipt in writing.

(2) Additionally, Classified Information may be transmitted or transferred between a Swedish company and a Estonian owned company in the Kingdom of Sweden or a Estonian company and a Swedish owned company in the Republic of Estonia using the national transmission or transfer regulations applicable in the country in which the companies are based.

Releases may only take place between companies which hold the relevant facility and personnel security clearances (See Article 9 (1)) and where the information has been approved for release to the other country.

Article 7. Visits

(1) The prior approval of the NSA / DSA of the host country will be required in respect of visitors, including those on detached duty from the other country, where access to Classified Information or to defence establishments /defence contractor premises engaged in classified work is necessary. Requests for such visits will be submitted through the respective Embassies.

(2) Requests will include the following information:

(a) surname and first name of proposed visitor, date and place of birth, nationality and passport number;

(b) 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;

(c) certificate indicating the level of security clearance of the visitor; (d) name and address of the establishment, company or organisation to be visited;

(e) name and status of the person(s) to be visited, if known;

(f) purpose of the visit; and

(g) date and duration of the visit. In cases of recurring visits the total period covered by the visits should be stated.

(3) All visitors will comply with the security regulations of the host country.

(4) Visit requests should be submitted to the Recipient Party in accordance with the normal procedures of the Recipient Party. Short notice visits can be arranged in urgent cases by special, mutually determined, arrangements.

(5) In cases involving a specific project or a particular contract it may, subject to the approval of both Parties, be possible to establish recurring visitors lists. These lists will be valid for an initial period not exceeding twelve (12) months and may be extended for a further period of time (not to exceed twelve (12) months) subject to the prior approval of the Competent Security Authority. They should be submitted in accordance with the normal procedures of the Recipient Party. Once a list has been approved, visit arrangements may be made direct between the establishments or companies involved in respect of listed individuals.

(6) Classified Information which may be provided to visiting personnel, or which may come to the notice of visiting personnel, will be treated by them as if such information had been furnished pursuant to the provisions of this Agrecment.

Article 8. Contracts

When proposing to place, or authorising a contractor in its country to place a Contract involving Classified Information with a Contractor in the other country the Originating Party will obtain prior clearance from the NSA / DSA of the other country that the proposed

Contractor is security cleared to the appropriate level and also has appropriate security measures to provide adequate protection for Classified Information. The security clearance will carry a responsibility that the security conduct by the cleared Contractor will be in accordance with national security rules and regulations and monitored by his NSA / DSA.

(2) The Competent Security Authority will ensure that Contractors that receive Contracts placed as a consequence of these pre-contract enquiries are aware of the following provisions:

(a) the definition of the term Classified Information and of the equivalent levels of security classification of the two Parties in accordance with the provisions of this Agreement;

(b) the names of the Government Authority of each of the two countries empowered to authorise the release and to co-ordinate the safeguarding of Classified Information related to the Contract;

(c) the channels to be used for the transmission or transfer of the Classified Information between the Government Authorities and / or Contractors involved;

(d) the procedures and mechanisms for communicating the changes that may arise in respect of Classified Information either because of changes in its Security Classification or because protection is no longer necessary;

(e) the procedures for approval of visits, access or inspection by personnel of one country to companies of the other country are covered by the Contract;

(f) an obligation that the Contractor will disclose the Classified Information only to a person who has previously been cleared for access and who has a "need to know", and is employed on or engaged in, the carrying out of the Contract;

(g) an obligation that the Contractor will not disclose the Classified Information or permit it to be disclosed to any person not expressly cleared in writing by the Contractor's NSA / DSA to have such access; and

(h) an obligation that the Contractor will immediately notify the Contractor's NSA / DSA or any actual or suspected breach or compromise of the Classified Information of this Contract.

(3) The Competent Security Authority of the Originating Party will pass two copies of the relevant parts of the Classified Contract to the Competent Security Authority of the Recipient Party, to allow adequate security monitoring.

(4) Each contract will contain guidance on the security requirements and on the classification of each aspect / elements of the Contract. In Sweden this guidance will be set out in separate security agreements. The guidance must identify each classified aspect of the Contract, or any classified aspect which is to be generated by the contract, and allocate to it a specific security classification. Changes in the requirements or to the aspects / elements will be notified as and when necessary and the Originating Party will notify the Recipient Party when all the information has been declassified.

Article 9. Reciprocal Industrial Security Arrangements

(1) Each NSA / DSA will notify the security status of a company's premises in its country when requested by the other Party. Each NSA / DSA will also notify the security clear-

ance status of one of its nationals when so requested. These notifications will be known as Facility security clearance (FSC) and Personnel security clearance (PSC) respectively.

(2) When requested the NSA / DSA will establish the security clearance status of the company / individual which is the subject of the inquiry and forward a security clearance if the company / individual is already cleared. If the company / individual does not have a security clearance, or the security clearance is at a lower security level than that which has been requested, notification will be sent that the security clearance cannot be issued immediately but that action is being taken to process the request. Following successful enquires a security clearance will be provided which will then permit a reciprocal security clearance to be issued.

(3) A company which is deemed by the NSA / DSA, in the country in which it is registered, to be under the ownership, control or influence of a third country whose aims are not compatible with those of the host Government is not eligible for a security clearance and the requesting NSA / DSA will be notified.

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

(5) If information becomes available which raises doubts about the suitability of a reciprocally cleared company to continue to have access to Classified Information in the other country then details of this information will be promptly given to the NSA / DSA to allow an investigation to be carried out.

(6) If either NSA / DSA suspends or takes action to revoke access which is granted to a national of the other country based upon a security clearance, the other Party will be notified and given the reasons for such an action.

(7) Each NSA / DSA may request the other to review any FSC, provided that their request is accompanied by the reasons for seeking such a review. Following this review, the requesting authority will be notified of the results and will be provided with facts supporting any decisions taken.

(8) If required by the other Party each NSA / DSA will cooperate in reviews and investigations concerning FSC and PSC.

Article 10. Implementation of Security Requirements

Implementation of security requirements can be advanced through reciprocal visits by security representatives of the Parties. Accordingly, security representatives of the Parties, after prior consultation, will be permitted to visit the other Party, to discuss the security system of the other Party.

Article 11. Breach or Compromise

(1) In the event of a security breach involving loss of Classified Material or suspicion that Classified Information has been disclosed to unauthorised persons, the NSA / DSA of the Recipient Party will immediately inform the NSA / DSA of the Originating Party in writing.

(2) An immediate investigation will be carried out by the Recipient Party (with assistance from the Originating Party if required) in accordance with the laws and regulations in force in that country for the protection of Classified Information. The Recipient Party will inform the Originating Party about the circumstances, measures adopted and outcome of the investigations as soon as possible.

Article 12. Costs

All costs incurred by one Party in the application of the obligations in this Agreement shall be borne by that Party.

Article 13. Amendments

This Agreement may be amended or supplemented in an annex after written consent by the Parties.

Article 14. Disputes

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

Article 15. Termination / Review

(1) This Agreement will remain in force until terminated by either Party giving the other Party six (6) months written notice of termination. Both Parties will remain responsible after termination for the safeguarding of all Classified Information exchanged under the provisions of this Agreement.

(2) Similarly, all Classified Information which is exchanged under this Agreement will be safeguarded, even though its transfer may occur after notice by either of the Parties to terminate.

(3) In the event of termination, solutions to any outstanding problems will be sought by consultations between the Parties.

(4) This Agreement will be reviewed by the Parties within ten (10) years after its effective date or as agreed when necessary.

Article 16. Effective Date

This Agreement will enter into force upon signature of both Parties.

Article 17. Signatures

(1) The foregoing represents the undertakings between the Republic of Estonia and the Kingdom of Sweden upon matters referred to therein.

(2) This Agreement is signed in two originals in the Estonian, Swedish and English language, all three texts equally authentic. In ease of different interpretation of this Agreement the English text will prevail.

Tallinn 30.01.2002

For the Republic of Estonia:
SVEN MIKSER

For the Kingdom of Sweden:
BJÖRN VON SYDOW

[ESTONIAN TEXT — TEXTE ESTONIEN]

EESTI VABARIIGI
JA
ROOTSI KUNINGRIIGI
ÜLDINE SALASTATUD TEABE KAITSE
JULGEOLEKUKOKKULEPE

SISUKORD

Eesti Vabariik ja Rootsi Kuningriik, edaspidi nimetatud "pooled", on oma riikliku julgeoleku huvides sõlminud käesoleva üldise julgeolekukokkuleppe eesmärgiga kaitsta heakskiidetud kanalite kaudu kahe maa vahel edastatavat salastatud teavet, mida edastatakse mõlema maa kaitsealase uurimistöö, tootmise ja hangete eesmärgil või kummagi maa äri- ja tööstusorganisatsioonide jaoks.

Käesolevat kokkulepet tõlgendatakse lähtuvalt riiklikest õigusaktidest.

ARTIKKEL 1
MÕISTED

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 või disketi kujul või muus vormis (nt lindistus, magnetsalvestis, perfokaart, lint jms).
- "**Lepingupartner**" tähendab füüsilist või juriidilist isikut, kellel on õigus sõlmida lepingut.
- "**Leping**" tähendab kokkulepet ühe või mitme osapoole vahel, mis loob ja määratleb pooltevahelisi kehtivaid õigusi ja kohustusi.
- "**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 pool**" 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.
- "**Salastatuse tasemed**" ja nende ekvivalendid mõlemal maal on:

Eestis	**Rootsis**
TÄIESTI SALAJANE	KVALIFICERAT HEMLIG
SALAJANE	HEMLIG
KONFIDENTSIAALNE	HEMLIG

Rootsi salastatud teave, mida edastatakse Eesti Vabariiki, tuleb, kus iganes võimalik märgistada nii Rootsi salastatuse tasemega, kui ka sellele vastava Eesti salastatuse tasemega.

Vajadusel võib kumbki pool paluda teist poolt osutada teabele omistatud salastatuse tasemest kõrgemal tasemel kaitset. Madalamal tasemel kaitset ei saa osutada.

ARTIKKEL 2
PÄDEVAD ASUTUSED

Pädevad julgeolekuasutused, kes vastutavad kaitsealase julgeoleku eest mõlemal maal on:

ROOTSIS

Pädev asutus, kes Rootsis vastutab kaitsealase julgeoleku eest on

Försvarsmakten
(Rootsi relvajõud)
Peakorter
Sõjaväeluure ja julgeolek (MUST)
SE-107 86 STOCKHOLM
Rootsi
Telefon: 46 8 788 7500
Faks: 46 8 788 8263

Määratud julgeolekuasutus Rootsis, kes vastutab kaitsealase materjaliga seotud riigikaitsealase julgeoleku eest on:

Försvarets Materielverk
(Rootsi kaitsealaste materjalide administratsioon)
Julgeolek
SE-115 88 STOCKHOLM
Rootsi
Telefon: 46 8 782 4000
Faks: 46 8 660 2251

EESTIS

Pädev asutus Eestis, kes on vastutav riigikaitsealase julgeoleku eest:

Riigisaladuse kaitse osakond
Kaitseministeerium
Sakala 1
15094 Tallinn
EESTI
Telefon: 372 640 6030
Faks: 372 640 6002

ARTIKKEL 3
KASUTAMISE JA AVALIKUSTAMISE PIIRANGUD

(1) Vastuvõtjad ei avalikusta ja ei kasuta salastatud teavet ning ei luba selle avalikustamist või kasutamist ilma eelnevate konsultatsioonideta, välja arvatud teavet edastava poole poolt näidatud eesmärkidel ja ulatuses.

(2) Teavet vastuvõttev pool ei anna edasi või ei avalikusta valitsusametnikule, lepingupartnerile või lepingupartneri töötajale või ükskõik millisele teisele isikule, kes on kolmanda maa kodanik või ükskõik millisele rahvusvahelisele organisatsioonile mitte mingisugust salastatud teavet, mis on vahetatud käesoleva lepingu kohaselt ega ei avalikusta üldsusele ilma edastava poolega konsulteerimata mingit osa salastatud teabest.

(3) Käesolev kokkulepe ei sisalda midagi, mis reguleeriks autoriõiguste loovutamist, kasutamist, vahetamist või avalikustamist või mida saaks võtta kui volitust selleks, kuni ei ole eelnevalt saadud spetsiaalset volitust nende õiguste omanikult, olenemata kas omanik on üks pooltest või on ta kolmas isik.

ARTIKKEL 4
SALASTATUD TEABE KAITSE

(1) Teavet edastav pool peab kindlustama, et teavet vastuvõttev pool on informeeritud:

(a) teabe salastatuse tasemest ja ükskõik millistest täiendavatest tingimustest selle avalikustamisel või kasutamise piirangutest ja et dokumendid on sellisena märgistatud; ja

(b) igast hilisemast salastatuse taseme muutusest.

(2) Teavet vastuvõttev pool peab:

(a) võimaldama vastavuses oma riiklike õigusaktidega salastatud teabele samasuguse kaitse nagu teabe edastaja. Teavet vastuvõttev pool peab ükskõik millisel õiguslikult lubataval viisil hoidma edastatud salastatud teavet avalikustamise eest ükskõik millisel õiguslikul alusel; ja kumbki pool peab tagama arvestuse ja kontrolli protseduurid korraldamaks salastatud teabe jaotamist ja juurdepääsu sellele.

(b) Tagama, et salastatud teave on märgistatud vastavuses artikliga 1; ja

(c) Tagama, et salastatuse taset muudetakse ainult teavet edastanud poole või tema esindaja kirjalikul loal.

(3) Saavutamaks ja hoidmaks julgeoleku võrreldavaid standardeid peab iga pädev asutus / julgeolekuasutus esitama nõudmisel teisele informatsiooni oma julgeolekustandardite, protseduuride ja salastatud teabe kaitse praktika kohta ja sel eesmärgil võimaldama pädevate asutuste visiite.

ARTIKKEL 5
JUURDEPÄÄS SALASTATUD TEABELE

Salastatud teabele juurdepääsu võib lubada neile isikutele, kellel on "põhjendatud teadmisvajadus" ja kes on läbinud asjaomase pädeva asutuse / julgeolekuasutuse julgeolekukontrolli, mis on vastavuses tema riiklike standarditega ja vastab selle teabe tasemele, millele juurdepääsu võimaldatakse.

ARTIKKEL 6
SALASTATUD TEABE EDASTAMINE

(1) Salastatud teavet edastatakse kahe maa vahel vastavalt teavet edastava poole riiklikele julgeolekujuhenditele. Üks võimalus on teha seda ametlike valitsusvaheliste diplomaatiliste kanalite kaudu, aga võib kasutada ka teisi viise, nagu käsipost, turvatud teabeedastus (krüpteerimine), kui see on vastastikku vastuvõetav mõlemale poolele. Salastatud teavet vastuvõttev pool peab teabe vastuvõtmisest kirjalikult teatama.

(2) Lisaks sellele võib salastatud teavet edastada Rootsi äriühing ja Eesti omanduses olev äriühing Rootsi Kuningriigis või Eesti äriühing ja Rootsi omanduses olev äriühing Eesti Vabariigis, kasutades riiklike teabe edastamise juhiseid, mis on kasutusel ettevõtte asukohamaal. Edastamine võib aset leida ainult nende ettevõtete vahel, millel on asjakohased asutuse ja isikute riigisaladusele juurdepääsu load (vt. artikkel 9 (1)) ja kui on antud nõusolek selle teabe edastamiseks teise riiki.

ARTIKKEL 7
VISIIDID

(1) Külastajate, kaasa arvatud teisest riigist teenistusse lähetatute suhtes, kellel on vajadus juurdepääsuks salastatud teabele või riigikaitseliste asutuste / salajasele koostööle kaasatud lepingupartneri territooriumile, on vajalik vastuvõtva riigi pädeva asutuse / julgeolekuasutuse nõusolek. Selliste visiitide taotlused esitatakse asjaomaste saatkondade kaudu.

(2) Visiiditaotlus peab sisaldama:

- külastaja perekonna- ja eesnime, andmeid sünnikoha ja –kuupäeva, kodakondsuse kohta ning passinumbrit;
- andmeid külastaja ametikoha kohta ning selle asutuse, ettevõtte või organisatsiooni nime, mida külastaja esindab või kuhu ta kuulub;
- tõendit, mis näitab külastaja juurdepääsuloa taset;
- külastatava asutuse, ettevõtte või organisatsiooni nime ning aadressi;
- Külastatava(te) isiku(te) nime ja ametikohta, kui need on teada;
- visiidi eesmärki;
- saabumis- ja lahkumisaega ning visiidi kestvust. Korduvate visiitide korral peab näitama ajavahemiku, mille jooksul visiidid toimuvad;

(3) Kõik külastajad peavad järgima vastuvõtva riigi julgeolekunõudeid.

(4) Visiiditaotlused tuleb esitada vastuvõtvale poolele vastavalt vastuvõtva poole protseduuridele. Lühikese etteteatamistähtajaga visiite on võimalik korraldada edasilükkamatutel juhtudel eriliste vastastikku määratletud kokkulepete alusel.

(5) Eriprojekti või konkreetset lepingut puudutavatel juhtudel on võimalik kummagi poole heakskiidul luua korduvate külastajate nimekirju. Nimekirjad võivad algselt kehtida perioodi vältel, mis ei ületa kahteteist (12) kuud ja neid võib pikendada lisaperioodiks (mis ei tohi ületada kahteteist (12) kuud), pikendamine toimub pädeva asutuse eelneva nõusoleku alusel. Nimekirjad tuleb esitada vastavuses vastuvõtva poole protseduuridega. Kui nimekiri on heaks kiidetud, võivad need asutused ja äriühingud, kelle esindajad on selles nimekirjas, visiitide suhtes kokku leppida otse.

(6) Külastajad peavad käsitlema salastatud teavet, mida võidakse neile anda või mis võib neile teatavaks saada, nii, nagu oleks see teave edastatud vastavalt käesoleva kokkuleppe tingimustele.

ARTIKKEL 8
LEPINGUD

(1) Kui tehakse ettepanek sõlmida või riik volitab lepingupartnerit sõlmima salastatud teavet puudutavat lepingut teises riigis asuva lepingupartneriga, siis teavet edastav pool peab saama eelneva kinnituse teise riigi pädevalt asutuselt / julgeolekuasutuselt, et pakutav lepingupartner on läbinud asjakohasel tasemel julgeolekukontrolli ja tal on kasutusel asjakohased julgeolekumeetmed tagamaks salastatud teabele vajalikku kaitset. Juurdepääsuluba tähendab vastutust selle eest, et kontrollitud lepingupartner on korraldanud julgeoleku vastavuses riiklike julgeolekut reguleerivate seaduste ja määrustega ning ta on tema pädeva asutuse / julgeolekuasutuse järelevalve all.

(2) Pädev asutus peab tagama, et lepingupartnerid, kes sõlmivad nende lepingueelsete uuringute tagajärjel lepingu, on teadlikud järgnevatest sätetest:

(a) Salastatud teabe mõistest ja vastavuses käesoleva lepingu tingimustele kahe poole võrreldavatest salastatuse tasemetest;

(b) Kummagi maa valitsusasutuste, kellel on volitused edastada ja koordineerida lepinguga seotud salastatud teabe kaitset, nimedest;

(c) Valitsusasutuste ja / või lepingupartnerite vahel salastatud teabe edastamiseks kasutatavatest kanalitest;

(d) Salastatud teabega seotud muudatuste tekkimisel neist teatamise protseduuridest ja mehhanismidest nii salastatuse tasemete muutmisel kui kaitsevajaduse äralangemisel;

(e) Visiitide, juurdepääsu või ühe poole töötajate poolt teise poole ettevõtetesse tehtavate inspektsioonide heakskiitmise lepingus sisalduvatest protseduuridest;

(f) Kohustusest, et lepingupartner avalikustab salastatud teavet ainult isikule, kes on eelnevalt läbinud julgeolekukontrolli, kellel on "põhjendatud teadmisvajadus" ja kes on töösuhetes või muul viisil seotud lepingu täitmisega.

(g) Kohustusest, et lepingupartner ei avalikusta salastatud teavet või ei luba selle avalikustamist ühelegi isikule, kellele ei ole selgesõnaliselt kirjalikult lubanud sellist juurdepääsu lepingupartneri pädev asutus / julgeolekuasutus;

(h) Kohustusest, et lepingupartner peab viivitamata teavitama lepingupartneri pädevat asutust / julgeolekuasutust igast toimunud või oletatavast julgeolekumeetmete rikkumisest või lepingus sisalduva salastatud teabe lekkest.

(3) Teavet edastava poole pädev asutus peab andma teavet vastuvõtva poole pädevale asutusele kaks koopiat salastatud lepingu asjassepuutuvatest osadest, võimaldamaks küllaldast julgeolekualast järelevalvet.

(4) Kõik lepingud peavad sisaldama julgeolekunõuete ja lepingu iga osa salastamise juhiseid. Rootsis antakse sellised juhised eraldi julgeolekukokkuleppega. Juhised peavad määratlema lepingu iga salastatud osa või salastatud osa, mis luuakse lepingu alusel, ja määrama sellele eraldi salastatuse taseme. Muudatustest nõudmistes või lepingu osades antakse teada igal ajal, kui see on vajalik ja teavet edastav pool peab teavitama teavet vastuvõtvat poolt, kui kogu see informatsioon kaotab oma salastatuse.

ARTIKKEL 9
VASTASTIKUSED TÖÖSTUSJULGEOLEKUALASED KORRALDUSED

(1) Iga pädev asutus / julgeolekuasutus peab teavitama teist poolt viimase nõudmisel oma riigis asuva äriühingu territooriumi julgeolekualasest staatusest. Iga pädev asutus / julgeolekuasutus peab samuti teatama iga oma kodaniku juurdepääsuloa tasemest, kui seda nõutakse. Need teated käsitletakse vastavalt asutuse juurdepääsuloana (FSC) ja üksikisiku juurdepääsuloana (PSC).

(2) Kui nõutakse, siis pädev asutus / julgeolekuasutus määrab kindlaks taotluses toodud äriühingu / üksikisiku juurdepääsuloa staatuse ja edastab juurdepääsuloa, kui äriühing/ üksikisik on juba kontrollitud. Kui äriühing / üksikisik ei oma juurdepääsuluba, või juurdepääsuluba on nõutavast madalama tasemega, tuleb saata teade, et juurdepääsuluba ei saa koheselt välja anda, aga taotluse rahuldamisega on asutud tegelema. Edukate järelepärimiste tulemusel väljastatakse juurdepääsuluba, mis võimaldab vastastikust juurdepääsulubade väljaandmist.

(3) Äriühing, mis oma asukohamaa pädeva asutuse /julgeolekuasutuse arvates on kolmanda riigi, mille eesmärgid on vastuolus asukohamaa huvidega, mõju all, ei vasta juurdepääsuloa saamise eeltingimustele ja sellest teavitatakse taotluse esitanud pädevat asutust /julgeolekuasutust.

(4) Kui kumbki pädev asutus / julgeolekuasutus saab ükskõik millist kahjustavat teavet isiku kohta, kellele on antud üksikisiku juurdepääsuluba, siis teavitab ta teist pädevat asutust / julgeolekuasutust informatsiooni iseloomust ja oma kavatsevast tegevusest või sellest, mida ta on ette võtnud. Põhjendatud taotluse korral võib kumbki pädev asutus / julgeolekuasutus nõuda teise pädeva asutuse/ julgeolekuasutuse poolt iga eelnevalt väljastatud üksikisiku juurdepääsuloa ülevaatamist. Taotluse esitanud pädevat asutust / julgeolekuasutust teavitatakse ülevaatamise tulemustest ja igast sellele järgnenud tegevusest.

(5) Kui saadakse informatsiooni, mis tekitab kahtlusi vastastikku juurdepääsuloa saanud äriühingu sobivusse saada salastatud teabele jätkuvalt juurdepääsu teises riigis, siis antakse selle informatsiooni detailid koheselt pädevale asutusele / julgeolekuasutusele uurimise läbiviimiseks.

(6) Kui kumbki pädev asutus / julgeolekuasutus peatab teise maa kodanikule juurdepääsuloa alusel antud juurdepääsu lubamise või astub samme juurdepääsu tühistamiseks, teavitatakse teist poolt ja põhjendatakse sellist tegevust.

(7) Iga lepingupartneri pädev asutus / julgeolekuasutus võib nõuda, et teine kontrolliks ükskõik millise asutuse juurdepääsuloa, tagades, et taotlusele on lisatud sellise kontrolli nõude põhjendus. Sellise nõudmise täitmisel teavitatakse nõude esitanud ametiasutust kontrolli tulemustest ja otsustamise aluseks olnud faktidest.

(8) Kui teine pool nõuab, siis peab iga pädev asutus / julgeolekuasutus tegema üksikisiku juurdepääsuloa ja asutuse juurdepääsuloa ülevaatamise ja kontrolli alal koostööd.

ARTIKKEL 10
JULGEOLEKUMEETMETE RAKENDAMINE

Julgeolekumeetmete rakendamist on võimalik edendada poolte julgeolekuesindajate vastastikuste visiitide kaudu. Vastavalt lubatakse poolte julgeoleku esindajatel pärast eelnevaid konsultatsioone külastada teist poolt, et arutada teise poole julgeolekusüsteemi.

ARTIKKEL 11
JULGEOLEKUMEETMETE RIKKUMINE VÕI TEABELEKE

(1) Kui julgeolekumeetmete rikkumisega kaasnes salastatud materjali kaotsiminek või kahtlus, et salastatud teave on saanud teatavaks volitamata isikutele, peab

teavet vastuvõtva poole pädev asutus / julgeolekuasutus teavet edastava poole pädevat asutust / julgeolekuasutust kirjalikult informeerima.

(2) Teavet vastuvõttev pool (kui nõutakse, siis teavet edastava poole abil) viib läbi viivitamatu uurimise vastavalt tema salastatud teabe kaitseks kehtivatele õigusaktidele ja juhenditele. Teavet vastuvõttev pool peab teavitama teavet edastavat poolt asjaoludest, tarvidusele võetud meetmetest ja uurimistulemusest niipea, kui võimalik.

ARTIKKEL 12
KULUD

Kõik ühe poole poolt käesoleva lepingu nõuete täitmisel tehtud kulud katab seesama pool.

ARTIKKEL 13
MUUTMINE

Kokkulepet võidakse poolte kirjalikul nõusolekul muuta või lisaga täiendada.

ARTIKKEL 14
ERIMEELSUSED

Kokkuleppe tõlgendamisest või rakendamisest tulenevad mistahes erimeelsused lahendatakse poolte vaheliste konsultatsioonide teel ja neid ei anta ühelegi riigisisesele või rahvusvahelisele kohtule või kolmandale poolele lahendamiseks.

ARTIKKEL 15
LÕPETAMINE/ ÜLEVAATAMINE

(1) Kokkuleppe on jõus, kuni üks pool selle lõpetab, teavitades teist poolt kuus (6) kuud kirjalikult ette. Mõlemad pooled jäävad vastutavaks kogu käesoleva kokkuleppe sätete kohaselt vahetatud salastatud teabe kaitse eest peale lepingu lõpetamist.

(2) Samaselt kaitstakse kogu käesoleva kokkuleppe kohaselt vahetatud salastatud teavet, isegi kui selle edastamine leidis aset pärast ükskõik kumma poole poolt edastatud lõpetamise teatist.

(3) Lõpetamise korral otsitakse kõigile lahendamata probleemidele lahendeid poolte vaheliste konsultatsioonide kaudu.

(4) Pooled vaatavad kokkuleppe üle kümne (10) aasta jooksul pärast kehtima hakkamist või kui lepitakse kokku selle vajalikkuses.

ARTIKKEL 16
JÕUSTUMISE KUUPÄEV

Kokkulepe jõustub selle allakirjutamisel mõlema poole poolt.

ARTIKKEL 17
ALLKIRJASTAMINE

(1) Eelkirjutatu väljendab Eesti Vabariigi ja Rootsi Kuningriigi vahelisi kohustusi ülalpool viidatud küsimustes.

(2) Käesolev kokkulepe on koostatud kahes eksemplaris, eesti, rootsi ja inglise keeles, kusjuures kõik tekstid on võrdse jõuga. Käesoleva kokkuleppe erineva tõlgendamise korral võetakse aluseks inglisekeelne tekst.

Tallinn 30.01.2002

Eesti Vabariigi nimel

Rootsi Kuningriigi nimel

[SWEDISH TEXT — TEXTE SUÉDOIS]

Avtal mellan

Republiken Estland

och

Konungariket Sverige

om skydd av sekretessbelagd information

Innehåll

Inledning

Republiken Estland och Konungariket Sverige, nedan kallade *parterna*, har i den nationella säkerhetens intresse träffat detta avtal för att trygga skydd av sekretessbelagd information som förmedlas mellan de båda länderna via godkända kanaler för försvarsforskning, tillverkning och upphandling eller till affärsdrivande och industriella enheter i de båda länderna.

Detta avtal skall tolkas i enlighet med nationell lag.

Artikel 1
Definitioner

Följande definitioner införs härmed för tydlighetens skull:

- *sekretessbelagd information*: varje sekretessbelagt föremål; det kan vara muntlig eller visuell förmedling av sekretessbelagt innehåll eller elektrisk eller elektronisk överföring av ett sekretessbelagt meddelande eller material som i den nationella säkerhetens intresse måste vara undantaget från röjande och som måste skyddas mot att sättas i fara.

- *material*: omfattar alla enheter av maskineri, utrustning eller vapen, såväl redan tillverkade som under tillverkning eller i form av handling.

- *handling*: varje informationsbärare som innehåller sekretessbelagd information, innefattande men inte begränsat till skrivelse, anteckning, protokoll, redogörelse, promemoria, signal, meddelande, teckning, fotografi, film, karta, grafisk framställning, anteckningsbok, stencil, karbonpapper, skrivmaskinsband, diskett, med mera eller annan form av bevarad information (exempelvis bandinspelning, magnetisk upptagning, hålkort och ljudband).

- *leverantör*: en fysisk eller juridisk person som är behörig att ingå avtal med rättsligt bindande verkan.

- *kontrakt*: en överenskommelse mellan två eller flera parter som skapar och definierar verkställbara rättigheter och skyldigheter mellan parterna.

- *sekretessbelagt kontrakt*: ett kontrakt som innehåller eller föranleder sekretessbelagd information.

- *nationell säkerhetsskyddsmyndighet (NSM) / behörig säkerhetsskyddsmyndighet (BSM)*: den statliga myndighet i vartdera landet som är ansvarig för försvarsmaktens säkerhetsskydd.

- *ursprungspart*: den part som är upphovsman till den sekretessbelagda information för vilken NSM/BSM är ansvarig.

- *mottagarpart*: den part till vilken den sekretessbelagda information förmedlas eller överförs för vilken NSM/BSM är ansvarig.

- *sekretessbeteckningar* och deras motsvarigheter i de båda länderna är följande:

Estland	Sverige
TÄIESTI SALAJANE	KVALIFICERAT HEMLIG
SALAJANE	HEMLIG
KONFIDENTSIAALNE	HEMLIG

Svensk sekretessbelagd information som skall förmedlas och överföras till Estland skall, där så är möjligt, märkas både med svensk sekretessbeteckning och motsvarande estländsk sekretessbeteckning.

Vid behov får den ena parten begära att den andra parten ger sekretesskydd på högre men inte på lägre nivå än den angivna sekretessnivån.

Artikel 2
Behöriga säkerhetsskyddsmyndigheter

Behöriga statliga myndigheter för försvarsmaktens säkerhetsskydd i respektive land är följande:

För Sverige

Den NSM som är ansvarig för försvarsmaktens säkerhetsskydd är Högkvarteret, Militär underrättelseverksamhet och säkerhet (MUST), adress: SE-107 86 Stockholm, telefon +46 8 788 75 00, fax +46 8 788 82 63.

Den BSM som är ansvarig för säkerhetsskyddet med avseende på försvarsmateriel är Försvarets materielverk, Säkerhetsskyddet, SE-115 88 Stockholm, telefon +46 8 782 40 00, fax +46 8 660 22 51.

För Estland

Den NSM som är ansvarig för försvarsmaktens säkerhetsskydd är följande: Security Department, Ministry of Defence, Sakala 1, 15094 Tallinn, ESTONIA Phone No +372 6406 030 Fax No +372 6406 002

Artikel 3
Inskränkningar i fråga om utnyttjande och röjande

1. Mottagarna får inte utan föregående samråd röja eller utnyttja eller tillåta röjande eller utnyttjande av sekretessbelagd information utom för de ändamål och med de begränsningar som angivits av ursprungsparten eller på dennas vägnar.

2. Mottagarparten får inte till en offentlig tjänsteman, en leverantör, dennes anställda eller någon annan person som är medborgare i tredje land, eller till internationell organisation förmedla eller röja sekretessbelagd information som den mottagit i

enlighet med bestämmelserna i detta avtal eller offentligen röja sekretessbelagd information utan föregående skriftligt tillstånd av ursprungsparten.

3. Ingen bestämmelse i detta avtal skall tolkas som ett bemyndigande eller vara bestämmande för att tillkännage, utnyttja, utväxla eller röja immateriell äganderätt förrän särskilt skriftligt tillstånd har erhållits av rättsinnehavaren, oberoende av om denna är en av parterna eller tredje man.

Artikel 4
Skydd av sekretessbelagd information

1. Ursprungsparten skall tillse att mottagarparten underrättas om

   a) informationens sekretessgrad och eventuella andra villkor för dess tillkännagivande eller begränsningar i fråga om utnyttjande och att informationen är märkt på detta sätt, samt

   b) eventuella senare ändringar av sekretessgrad.

2. Mottagarparten skall

   a) i enlighet med sina nationella lagar och bestämmelser ge sekretessbelagd information ett säkerhetsskydd som är likvärdigt med det skydd som ursprungsparten ger; mottagarparten skall vidare vidta alla åtgärder som lagligen står den till buds för att tillse att förmedlad och överförd sekretessbelagd information inte röjs med stöd av lagbestämmelser; vardera parten skall ha registrerings- och kontrollförfaranden för att hantera spridning av och tillgång till sekretessbelagd information,

   b) tillse att sekretessbelagd information åsätts dess egen sekretessbeteckning i enlighet med artikel 1, och

   c) tillse att sekretessbeteckningen inte ändras utan skriftligt tillstånd av ursprungsparten.

3. För att uppnå och bibehålla likvärdigt säkerhetsskydd, skall parternas NSM/BSM efter anmodan lämna varandra upplysningar om sina normer och förfaranden och sin praxis avseende skydd av sekretessbelagd information och skall i detta syfte underlätta besök från varandra.

Artikel 5
Rätt att ta del av sekretessbelagd information

Rätt att ta del av sekretessbelagd information skall vara förbehållen personer som har behov av den i tjänsten och som har genomgått säkerhetsklarering av NSM/BSM i mottagarparten i enlighet med dennas nationella normer för den sekretessnivå som motsvarar sekretessgraden hos den information varav del skall tas.

Artikel 6
Förmedling av sekretessbelagd information

1. Sekretessbelagd information skall förmedlas mellan de båda länderna i enlighet med ursprungspartens nationella säkerhetsskyddsföreskrifter. En kommunikationsväg är via de officiella diplomatiska kanalerna mellan de båda parterna, men andra arrangemang får upprättas, såsom genom personligt överlämnande eller via säkra kommunikationsmedel (såsom krypto), om de är godtagbara för båda parter. Mottagarparten skall skriftligen bekräfta mottagandet.

2. Sekretessbelagd information får dessutom förmedlas och överföras mellan ett svenskt företag och ett estländskägt företag i Sverige eller ett estländskt företag och ett svenskägt företag i Estland med tillämpning av de nationella reglerna för förmedlan och överföring som gäller i det land där företagen är baserade. Röjande får endast ske mellan företag som har genomgått erforderlig säkerhetsklarering för anläggningar och personer (se artikel 9.1) samt på villkor att informationen har godkänts för röjande till det andra landet.

Artikel 7
Besök

1. Förhandstillstånd av NSM/BSM i mottagarlandet erfordras för besökare, inbegripet besökare som är detacherade från det andra landet, i det fall tillgång till sekretessbelagd information eller tillträde till försvarsanläggningar eller till anläggningar tillhöriga leverantörer av sekretessbelagd försvarsmateriel erfordras. Framställning om tillstånd för sådana besök skall göras på diplomatisk väg.

2. En framställning skall innehålla följande upplysningar:

   a) Besökarens efternamn och förnamn, födelsetid, födelseort, medborgarskap och passnummer.

   b) Besökarens officiella ställning och namnet på den anläggning, det företag eller den organisation som besökaren företräder eller tillhör.

   c) Intyg som utvisar besökarens grad av säkerhetsklarering.

   d) Namn och adress på den anläggning, det företag eller den organisation som skall besökas.

   e) Namn på den eller de personer som skall besökas och deras ställning, om dessa uppgifter är kända.

   f) Ändamålet med besöket.

   g) Besökets tidpunkt och längd. Vid återkommande besök skall hela besöksperioden anges.

3. Besökare är skyldiga att följa värdlandets säkerhetsskyddsbestämmelser.

4. Framställningar om besök bör överlämnas till mottagarparten i enlighet med dennas normala förfaranden. Besök med kort varsel kan i brådskande fall anordnas genom särskilda avtalade arrangemang mellan parterna.

5. I fråga om ett visst projekt eller kontrakt får det vara möjligt att, med båda parters godkännande, göra upp förteckningar över personer som skall göra återkommande besök. Sådana förteckningar skall gälla för en första period om högst tolv månader som får förlängas, dock ej längre tid än tolv månader efter förhandsgodkännande av den behöriga säkerhetsskyddsmyndigheten. Förteckningarna bör överlämnas i enlighet med mottagarpartens normala förfaranden. När en förteckning har godkänts, får besöksarrangemangen göras upp direkt mellan de berörda anläggningarna eller företagen med avseende på personer som står upptagna i förteckningen.

6. Sekretessbelagd information som kan lämnas till besökare, eller som kan komma till deras kännedom, skall av dem behandlas som mottagen i enlighet med bestämmelserna i detta avtal.

Artikel 8
Kontrakt

1. När ursprungsparten avser att göra en beställning, eller bemyndigar en leverantör i sitt land att göra en beställning, som innefattar sekretessbelagd information hos en leverantör i det andra landet, skall den i förväg begära säkerhetsklarering från NSM/BSM i det andra landet som utvisar att den avsedda leverantören är säkerhetsklarerad upp till den erforderliga nivån och har tillräckliga säkerhetsanordningar för att ge sekretessbelagd information erforderligt skydd. I intyget om säkerhetsklarering skall ingå en försäkran att den klarerade leverantörens sekretessbeteende skall stå i överensstämmelse med nationella sekretesslagar och bestämmelser och övervakas av dennas NSM/BSM.

2. Den behöriga säkerhetsskyddsmyndigheten skall tillse att leverantörer som får beställningar till följd av dessa förkontraktuella undersökningar är vederbörligen informerade om följande:

   a) Definitionen av termen *sekretessbelagd information* och likvärdiga nivåer ör sekretessbeteckningar i de båda parterna enligt detta avtal.

   b) Namnen på de båda ländernas myndigheter som är behöriga att ge tillstånd till röjande av och samordning av skyddet av sekretessbelagd information som rör ett kontrakt.

   c) Kanaler som skall användas för förmedling eller överföring av sekretessbelagd information mellan de berörda myndigheterna och/eller leverantörerna.

d) Förfaranden och mekanismer för att meddela eventuella förändringar gällande sekretessbelagd information, antingen när det gäller sekretessbeteckning eller att skydd inte längre behövs.

e) Formaliteter för beviljande av besökstillstånd, tillträde eller inspektion för personer från det ena landet avseende företag i det andra landet som omfattas av ett kontrakt.

f) Att leverantören förbinder sig att inte röja sekretessbelagd information till andra personer än sådana som har säkerhetsklarerats med avseende på rätt att ta del av informationen, som har behov av den i tjänsten och som är anställda eller anlitade för att genomföra ett kontrakt.

g) Att leverantören förbinder sig att inte röja sekretessbelagd information eller tillåta att sådan information röjs för personer som saknar skriftligt tillstånd att ta del av den utfärdat av personens NSM/BSM.

h) Att leverantören är skyldig att omedelbart meddela sin NSM/BSM verklig eller befarad förlust eller läcka av sekretessbelagd information som hör till ett kontrakt eller om informationen har utsatts för fara.

3. Den behöriga säkerhetsskyddsmyndigheten i ursprungsparten skall överlämna två kopior av de berörda delarna av ett sekretessbelagt kontrakt till mottagarpartens behöriga säkerhetsskyddsmyndighet för att möjliggöra erforderlig säkerhetsövervakning.

4. Varje kontrakt skall innehålla anvisningar om sekretessbestämmelserna och sekretessbeteckningarna för varje aspekt eller del av ett kontrakt. För Sveriges del skall dessa anvisningar anges i särskilda säkerhetsskyddsöverenskommelser. I anvisningarna måste varje sekretessbelagd aspekt av ett kontrakt identifieras, eller varje sekretessbelagd aspekt som kommer att genereras av detta, och åsättas en särskild sekretessbeteckning. Ändringar i krav, aspekter eller delar skall meddelas om och när så är nödvändigt. Ursprungsparten skall meddela mottagarparten när sekretessen för all information har upphävts.

Artikel 9
Ömsesidiga säkerhetsskyddsarrangemang för industrin

1. Vardera partens NSM/BSM skall på begäran av den andra parten lämna upplysningar om säkerhetsläget för ett företags lokaler i sitt land. NSM/BSM skall också på begäran lämna upplysningar om säkerhetsläget för sina medborgare. Dessa upplysningar benämns *säkerhetsklarering för anläggningar (SKA)* respektive *säkerhetsklarering för personer (SKP)*.

2. NSM/BSM skall på begäran fastställa status för säkerhetsklarering för företag eller person som är föremål för prövning och översända intyg om

säkerhetsklarering, om företaget eller personen redan är klarerad. Om företaget eller personen saknar intyg om säkerhetsklarering eller om klareringen gäller en lägre sekretessgrad än den som har begärts, skall upplysningar sändas med innebörd att intyg om säkerhetsklarering inte omedelbart kan utfärdas, men att åtgärder håller på att vidtas för att behandla framställningen. Om prövningen ger godkänt resultat, skall intyg om säkerhetsklarering utfärdas, vilket sedan skall medge att intyg om ömsesidig säkerhetsklarering utfärdas.

3. För ett företag som av NSM/BSM i det land där det är registrerat bedöms stå under ägande, kontroll eller inflytande av tredje land, vars syften inte är förenliga med värdpartens syften, får säkerhetsklarering inte utfärdas, och NSM/BSM skall underrättas.

4. Om någon av NSM/BSM får kännedom om någon nedsättande uppgift om en person för vilken en SKP har utfärdats, skall den meddela de andra NSM/BSM om uppgiftens karaktär och om de åtgärder den avser vidta eller har vidtagit. NSM/BSM får begära omprövning av en SKP som tidigare har lämnats av den andra behöriga säkerhetsskyddsmyndigheten, under förutsättning att framställningen åtföljs av en motivering. Den begärande NSM/BSM skall underrättas om resultatet av omprövningen och om därav föranledda åtgärder.

5. Om uppgifter framkommer som väcker tvivel om ett ömsesidigt godkänt företags lämplighet att fortsätta att få tillgång till sekretessbelagd information i det andra landet, skall närmare detaljer om dessa uppgifter ofördröjligen framföras till NSM/BSM för att möjliggöra en undersökning.

6. Om endera NSM/BSM upphäver eller vidtar åtgärder för att dra in ett tillstånd till tillträde som har beviljats en medborgare i det andra landet med stöd av en säkerhetsklarering, skall den andra parten underrättas och delges motiven för dessa åtgärder.

7. Den ena NSM/BSM får med en motiverad framställning begära att den andra omprövar en SKA. Den begärande säkerhetsskyddsmyndigheten skall efter omprövningen underrättas om resultatet av denna och delges de omständigheter som styrker ett eventuellt beslut.

8. Vardera partens NSM/BSM skall på begäran av den andra parten samarbeta vid omprövningar och undersökningar avseende SKA och SKP.

Artikel 10
Verkställande av säkerhetskrav

Verkställande av säkerhetskrav kan främjas genom ömsesidiga besök av parternas säkerhetsrepresentanter. Därför skall dessa efter samråd få tillåtelse att besöka varandra för att rådgöra om varandras säkerhetssystem.

Artikel 11
Förlust eller fara

1. I händelse av brott mot säkerheten som innebär förlust av sekretessbelagt material, eller misstanke om att sekretessbelagd information har röjts för obehöriga, skall mottagarpartens NSM/BSM omedelbart skriftligen underrätta ursprungspartens NSM/BSM.

2. Mottagarparten skall omedelbart genomföra en undersökning (med biträde av ursprungsparten om så erfordras) i enlighet med sina gällande lagar och bestämmelser om skydd av sekretessbelagd information. Mottagarparten skall, så snart det är praktiskt möjligt, underrätta ursprungsparten om omständigheterna, om vilka åtgärder som vidtagits samt om resultatet av undersökningen.

Artikel 12
Kostnader

Alla kostnader som förorsakas av en part vid fullgörande av åtagandena enligt detta avtal skall täckas av den parten.

Artikel 13
Ändringar

Detta avtal kan ändras eller förses med tillägg i en bilaga efter parternas skriftliga samtycke.

Artikel 14
Tvister

Tvister om tolkningen eller tillämpningen av detta avtal skall lösas genom samråd mellan parterna och inte hänskjutas till nationell eller internationell domstol eller tredje man för lösande.

Artikel 15
Uppsägning och översyn

1. Detta avtal skall förbli i kraft tills det skriftligen sägs upp av någon av parterna med sex månaders varsel. Sedan avtalet har upphört att gälla, skall båda parter vara ansvariga för skyddet av sekretessbelagd information som har utbytts i enlighet med dess bestämmelser.

2. Likaledes skall sekretessbelagd information som utväxlats med stöd av detta avtal skyddas, även om förmedlingen har skett efter det att någon av parterna har sagt upp avtalet.

3. I fall av uppsägning skall utestående frågor söka lösas genom samråd mellan parterna.

4. Parterna skall göra en översyn av detta avtal inom tio år efter dess ikraftträdande eller i mån av behov, om så överenskoms.

Artikel 16
Ikraftträdande

Detta avtal träder i kraft när båda parter undertecknar det.

Artikel 17
Undertecknande

1. Ovanstående motsvarar Konungariket Sveriges och Republiken Estlands åtaganden om frågor som täcks av detta avtal.

2. Detta avtal är undertecknat i två original på estniska, svenska och engelska språken, vilka alla tre texter är lika giltiga. I fall av skiljaktighet i fråga om tolkningen av detta avtal, skall den engelska texten ha företräde.

Tallinn 30.01.2002

För Republiken Estland:

För Konungariket Sverige:

[TRANSLATION — TRADUCTION]

ACCORD ENTRE LA RÉPUBLIQUE D'ESTONIE ET LE ROYAUME DE SUÈDE RELATIF À LA PROTECTION DES INFORMATIONS CLASSIFIÉES

Table des matières

Dans l'intérêt de la sécurité nationale et souhaitant assurer la protection des informations classifiées échangées entre les deux pays dans les recherches sur la défense, la production et les approvisionnements au bénéfice des organisations commerciales et industrielles des deux pays par des voies qu'ils ont approuvées, la République d'Estonie et le Royaume de Suède (ci-après dénommés les "Parties),ont établi un Accord global de sécurité. Le présent accord doit être interprété conformément à la législation nationale.

Article 1. Définitions

Les termes suivants sont définis dans l'intérêt de la clarté :

"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 sans limite.

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

"Document " s'entend de tout médium 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 .

"Entrepreneur" 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 de sécurité nationale (NSA) /Autorité désignée pour la sécurité (DSA) signifie toute autorité gouvernementale responsable de la sécurité de la défense dans chacun des pays.

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

"Partie destinataire" signifie Partie à laquelle l'information classifiée est transmise ou transférée, telle qu'elle est représentée par NSA/DSA.

"Les classifications de sécurité" et leur équivalent dans les deux pays sont :

En Estonie	En Suède
Täiesti Salajane	Kvalificerat Hemlig
Salajane	Hemlig
Konfidentsiaalne	Hemlig

L'information classifiée suédoise transmise ou transférée à la République d'Estonie sera, autant que possible, marquée par la classification de sécurité suédoise et la classification estonienne correspondante.

Dans certains cas, une partie peut demander à l'autre de fixer le niveau de classification à un niveau plus élevé que la classification indiquée. On ne peut pas demander un niveau de classification plus bas que la classification indiquée.

Article 2. Les autorités compétentes pour la sécurité

Les autorités gouvernementales compétentes pour la sécurité de la défense sont les suivantes:

Pour la Suède

La NSA en Suède responsable pour les questions de sécurité militaire est :

Försvarsmakten

Forces armées suédoises

Quartier général

Sécurité et renseignement militaire (MUST)

SE-107 86 Stockholm, Suède

Tel : +46 8 788 7500

Télécopie : +46 8 788 8263

La DSA en Suède responsable pour la défense de la sécurité associée à la défense du matériel est :

Försvarets Materielverk

(L'administration suédoise de la défense du matériel))

Sécurité

SE-115 88 Suède

Tel : +46 8 782 4000

Télécopie : +46 8 660 2251

En Estonie

La NSA en Estonie responsable pour la défense de la sécurité associée aux questions de défense de la sécurité est :

Département de la Sécurité

Ministère de la Défense

Sakala 1,15094

Tallinn, Estonie

Tel : +372 6406 030

Télécopie : +372 6406 002

Article 3. Restrictions à l'utilisation et à la divulgation des informations

1) La partie destinataire ne doit pas sans consultation préalable, divulguer, utiliser ou permettre que soit divulgué ou utilisé des informations classifiées à moins que cette divulgation soit effectuée dans des limites définies par la partie d'origine ou en son nom.

2) La partie destinataire ne communiquera pas à un responsable gouvernemental, à un entrepreneur, à ses employés ou à des personnes qui sont des ressortissants d'un pays tiers ou à une organisation internationale, une information classifiée qui a été échangée selon les dispositions du présent accord. Elle ne divulguera pas publiquement aucune information classifiée sans consultation préalable de la partie d'origine.

3) Aucune disposition du présent accord ne confère l'autorité à quiconque de diffuser, utiliser, divulguer des droits de propriété intellectuelle sans une autorisation spécifique écrite du propriétaire de ces droits; que le propriétaire soit ou non l'une des parties ou une tierce partie.

Article 4. Protection de l'information classifiée

1) La partie d'origine doit s'assurer que la partie destinataire est informée de :

a) la classifieation de l'information et des conditions additionnelles à sa diffusion ou aux limitations à son utilisation et que ces documents sont marqués ; et

(b) tout changement de la classification.

2) La partie destinataire doit :

a) conformément à ses lois et à ses règlements, accorder à l'information classifiée le niveau de protection que lui a accordé la partie d'origine. La partie destinataire prendra toutes les mesures qui sont disponibles légalement pour que l'information classifiée ne soit pas divulguée en vertu d'une quelconque disposition législative. Chacune des parties établira des procédures de responsabilité et de contrôle pour la gestion de la diffusion et l'accès à l'information classifiée ;

b) assurer que l'information classifiée est marquée conformément à l'article 1 ; et

c) assurer que la classification n'est pas altérée, à moins que la partie d'origine ou une partie agissant en son nom, n'ait autorisé cette altération par écrit.

3) Afin d'atteindre et de maintenir des normes de sécurité comparables, Chaque NSA/DSA, devra, sur demande, fournir l'une à l'autre des renseignements à propos des normes, procédures et pratiques pour protéger l'information classifiée et à cette fin, faciliter les visites des autorités compétentes pour la sécurité.

Article 5. Accès à l'information classifiée

L'accès aux informations classifiées doit être limité aux personnes "qui ont besoin de les connaître" ou qui ont reçu une habilitation de sécurité de la NSA/DSA selon leur norme nationale, au niveau de classification approprié pour l'information concernée.

Article 6. Transmission de l'information classifiée

1) Les informations classifiées seront transmises entre les deux pays conformément aux règlements concernant la sécurité nationale de la partie d'origine. La voie diplomatique est l'une des voies mais d'autres arrangements peuvent être envisagés tels transport à la main, communication sécurisée (chiffrement) si les deux parties l'acceptent. La partie destinataire de l'information doit fournir un accusé de réception.

2) En outre, l'information peut être transmise ou transférée d'une société suédoise à une société estonienne dans le Royaume de Suède ou d'une société estonienne à une société suédoise en Estonie en utilisant une transmission nationale ou des règles de transfert applicables dans le pays où les sociétés sont basées. La diffusion ne peut prendre place qu'entre des sociétés qui ont des installations appropriées et des habilitations de sécurité (voir alinéa 1 de l'article 9) et lorsque la diffusion de l'information dans un autre pays a été approuvée.

Article 7. Visites

1) L'approbation préalable de la NSA/DSA du pays hôte sera exigé pour les visiteurs y compris les visiteurs en mission de l'autre pays lorsque l'accès aux informations classifiées et aux installations de défense engagés dans le travail de classification est nécessaire. Les demandes de visites doivent être soumises aux ambassades des pays respectifs.

2) Les informations suivantes doivent figurer sur les demandes :

a) Nom et prénom du visiteur, date et lieu de naissance, nationalité et numéro de passeport ;

b) Statut officiel du visiteur ainsi que le nom de l'établissement, société ou organisation que le visiteur représente ou auquel il appartient ;

c) Certificat indiquant le niveau d'habilitation de sécurité du visiteur ;

d) Nom et adresse de l'établissement, société ou organisation qui doit être visité ;

e) Nom et statut des personnes auxquelles on rend visite, si c'est possible ;

f) But de la visite, et

g) Date et durée de la visite. En cas de visites répétées, la période totale couverte par les visites doit être indiquée.

3) Tous les visiteurs doivent respecter les règlements de sécurité du pays hôte.

4) Les demandes de visites doivent être soumises à la partie destinataire conformément aux procédures normales de la partie destinataire. Des visites dans de courts délais peuvent être décidées dans des cas urgents par des arrangements spéciaux mutuellement agréés.

5) Dans les cas où des projets spécifiques ou un contrat particulier sont pris en considération, il est possible sous réserve de l'approbation des deux parties d'établir des listes de visiteurs qui reviennent souvent. Ces listes sont valables pour une période initiale ne dépassant pas 12 mois et qui peut être prorogée pour une période supplémentaire (ne dépassant pas 12 mois) sous réserve de l'approbation préalable de l'autorité de sécurité compétente. Ces listes devraient être soumises conformément aux procédures normales de la partie destinataire. Une fois la liste approuvée, les arrangements en vue des visites peuvent être effectués directement entre les établissements et les sociétés intéressés par les personnes figurant sur la liste.

6) Les visiteurs doivent traiter les informations classifiées qui leur sont fournies ou sur lesquelles leur attention est attirée comme des informations correspondant aux dispositions du présent accord.

Article 8. Contrats

1) La partie d'origine doit obtenir l'approbation préalable en matière de sécurité de la NSA/DSA de l'autre partie si elle veut proposer ou autoriser un entrepreneur de son pays à passer un contrat qui touehe des informations classifiées avec un entrepreneur de cette autre partie. L'entrepreneur proposé doit avoir l'habilitation de sécurité au niveau approprié et doit pouvoir également assurer la protection adéquate des informations classifiées. L'habilitation de sécurité devra garantir que la conduite de l'entrepreneur habilité sera conforme aux normes et aux conduites en matière de sécurité supervisées par sa propre NSA/DSA.

2) Les autorités compétentes en matière de sécurité devront s'assurer que les entrepreneurs auxquels des contrats ont été consentis à la suite à d'enquêtes n'ignorent pas les dispositions suivantes :

a) la définition du terme information classifiée et les niveaux équivalents de classification de la sécurité des deux parties conformément aux dispositions du présent accord ;

b) les noms de l'Autorité gouvernementale des deux pays ayant le pouvoir d'autoriser la diffusion de l'information et de coordonner la sauvegarde des informations classifiées liées au contrat ;

c) les voies qui seront utilisées pour la transmission ou le transfert des informations classifiées entre les autorités gouvernementales et/ou les entrepreneurs impliqués ;

d) les procédures et les mécanismes pour communiquer les changements qui ont pu intervenir en ce qui concerne les informations classifiées, soit à cause de changements de la classification de sécurité soit parce que la protection n'est plus nécessaire ;

e) les procédures d'approbation des visites, d'accès ou d'inspection des sociétés d'un pays par le personnel de l'autre pays sont prévues par le contrat;

f) l'obligation de l'entrepreneur de divulguer les informations classifiées qu'à la personne qui est habilitée a en avoir accès et qui a "besoin de connaître" et qui dans le contrat, est employée ou engagée à cette fin.

g) l'obligation de l'entrepreneur de ne pas divulguer une information classifiée ou de ne pas permettre qu'elle soit diffusée à une personne qui n'a pas été habilitée par écrit par l'entrepreneur NSA/DSA; et

h) l'obligation de l'entrepreneur d'informer immédiatement l'entrepreneur NSA/DSA en cas de violation de la sécurité ou une compromission au sujet de l'information classifiée.

3) L'autorité compétente pour la sécurité de la partie d'origine communiquera deux copies des parties pertinentes du contrat à l'autorité compétente de la partie destinataire afin de faciliter un contrôle adéquat de la sécurité.

4) Dans chacun des contrats devront figurer des directives sur les exigences de sécurité et sur la classification de chaque élément du contrat. En Suède, les directives doivent figurer dans des accords séparés. Les directives doivent identifier chacun des aspects classifiés du contrat ou tout autre aspect qui en pourrait découler et leur allouer une classification spécifique de sécurité. Si des modifications sont apportées dans les demandes/exigences ou dans les éléments, elles devront être notifiées si nécessaire. La partie d'origine devra notifier à la partie destinataire toutes les informations déclassifiées.

Article 9. Arrangements réciproques de sécurité industrielle

1) Chaque NSA/DSA d'une partie devra notifier les conditions de sécurité des installations dans son pays si l'autre partie en fait la demande. Les notifications sont connues respectivement sous les termes d'habilitation de sécurité des installations (FSC) et d'habilitation de sécurité du personnel (PSC).

2) Sur demande, la NSA/DSA établira l'état de la sécurité de la société qui fait l'objet de l'enquête et transmettra une habilitation de sécurité si la société ou la personne est déjà habilitée. Si la société ou la personne n'ont pas l'habilitation de sécurité ou si l'habilitation est à un niveau inférieur à celui qui a été demandé, il sera nécessaire de notifier que l'habilitation de sécurité ne peut pas être délivrée immédiatement et que des mesures sont prises à cet effet. En cas de résultat positif, une habilitation de sécurité sera fournie qui permettra de délivrer une habilitation de sécurité réciproque.

3) Une société que la NSA/DSA considère être la propriété, sous le contrôle ou l'influence d'un pays tiers, dans le pays où elle est immatriculée et dont les buts ne sont pas compatibles avec ceux du pays hôte n'est pas qualifiée pour une habilitation de sécurité. La NSA/DSA qui en fait la demande devra en être notifiée.

4) Si l'une ou l'autre NSA/DSA est saisie d'une information désobligeante à propos d'une personne au bénéfice de laquelle une habilitation personnelle de sécurité a été délivrée, elle doit en informer l'autre NSA/DSA sur la nature de l'information et les mesures qu'elle a l'intention de prendre ou a déjà prises. L'une ou l'autre NSA/DSA peut demander un examen de l'habilitation précédemment fournie à condition que la demande soit fondée. Les résultats de l'examen et les mesures subséquentes qui seront prises seront communiqués à la NSA/DSA qui a fait la demande.

5) Si une information publiée introduit un doute quelconque sur l'opportunité pour une société qui a reçu de part et d'autre une habilitation de sécurité de continuer à avoir accès à des informations classifiées dans l'autre pays, les détails de cette information doivent être transmis immédiatement à la NSA/DSA afin qu'une enquête puisse être menée.

6) Si l'une ou l'autre NSA/DSA suspend ou prend des mesures pour révoquer l'accès accordé à un ressortissant de l'autre pays sur la base de l'habilitation de sécurité, l'autre partie doit en être informée et les motifs qui en sont à la base doivent lui être fournis.

7) Chacune des NSA/DSA peut demander à l'autre de réexaminer une habilitation des dispositifs de sécurité (FSC) à condition que les motifs de la demande soit indiqués. A la suite de cet examen, l'autorité requérante sera informée des résultats et des faits qui ont motivé la décision.

8) Si l'autre partie le demande, chacune des NSA/DSA peut participer aux enquêtes et à l'examen concernant les habilitations.

Article 10. Mise en oeuvre des mesures de sécurité

La mise en oeuvre des mesures de sécurité peut être effectuée grâce à des visites réciproques des employés chargés de la sécurité des parties. En conséquence, ces employés, après les consultations préalables seront autorisés à visiter l'autre partie pour discuter des systèmes de sécurité.

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

1) Dans le cas d'une violation de la sécurité entraînant la perte de la matière classifiée ou le doute qu'une information classifiée a pu être communiquée à des personnes non autorisées, la NSA/DSA de la partie destinataire doit en informer immédiatement la NSA/DSA de la partie d'origine par écrit.

2) Une enquête immédiate doit être déclenchée par la partie destinataire (avec la participation de la partie d'origine si elle est demandée) conformément aux lois et aux règlements en vigueur dans le pays pour la protection des informations classifiées. La partie destinataire informera la partie d'origine sur les circonstances et les mesures adoptées et les résultats de l'enquête le plus tôt possible.

Article 12. Coûts

Tous les frais encourus par une partie dans l'application des dispositions du présent accord seront à la charge de cette partie.

Article 13. Amendement

Le présent accord peut être modifié ou complété par une annexe après consentement écrit des parties.

Article 14. Différends

Tout différend concernant l'interprétation ou l'application du présent accord doit être résolu par voie de consultation entre les parties et ne sera pas référé à un tribunal national ou international ou à une tierce partie

Article 15. Dénonciation/Examen

1) Le présent accord restera en vigueur jusqu'à ce qu'il soit dénoncé par l'une ou l'autre des parties après un préavis écrit de six mois. Les deux parties continueront à être responsables de la sauvegarde de toutes les informations classifiées échangées selon les dispositions du présent accord.

2) De même, les informations classifiées échangées selon les dispositions de l'accord seront sauvegardées même si le transfert a eu lieu après la notification de dénonciation.

3) En cas de dénonciation, les solutions des problèmes en suspens seront cherchées par des consultations entre les parties.

4) Le présent accord sera examiné par les parties 10 ans après son entrée en vigueur ou à une date agréée, si nécessaire.

Article 16. Date d'entrée en vigueur

Le présent accord entre en vigueur à la date de la signature par les parties.

Article 17. Signatures

1) Les dispositions précédentes constituent des engagements de la République d'Estonie et du Royaume de Suède sur les questions de l'information classifiée.

2) Le présent accord est signé en deux copies originales en estonien, suédois et anglais, les trois textes faisant foi. En cas de divergence d'interprétation, le texte anglais prévaudra.

Pour la République d'Estonia :

SVEN MIKSER

Pour le Royaume de Suède :

BJÖRN VON SYDOW