

**Hallituksen esitys Eduskunnalle Tanskan, Suomen, Islannin, Norjan ja Ruotsin välillä turvallisuusluokitellun tiedon vastavuoroisesta suojaamisesta ja vaihtamisesta tehdyn yleisen turvallisuussopimuksen hyväksymisestä sekä laiksi mainitun sopimuksen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta**

**ESITYKSEN PÄÄASIALLINEN SISÄLTÖ**

Esityksessä ehdotetaan, että eduskunta hyväksyisi Tanskan, Suomen, Islannin, Norjan, ja Ruotsin välisen yleisen turvallisuussopimuksen turvallisuusluokitellun tiedon vastavuoroisesta suojaamisesta ja vaihtamisesta sekä lain sopimuksen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta.

Sopimuksen tarkoituksena on suojata turvallisuusluokiteltua tietoa, jota kaksi tai useampi sopimuspuolena oleva Pohjoismaa vaihtaa keskenään tai jota Pohjoismaiden lainkäyttövaltaan kuuluvat hankeosapuolet vaihtavat keskenään ulko-, puolustus-, turvallisuus- ja poliisiasioissa tai tiede-, elinkeino- ja teknologiayhteistyössä tai jota tuotetaan tai syntyy vaihdettavan tiedon perusteella. Kysymys on erityissuojattavista tietoaineistoista, jotka lähetävässä sopimusvaltiossa on erikseen luokiteltu korkeaa tietoturvallisuuden tasoa edellyttäväksi.

Sopimus tulee voimaan kolmantenakymmenentenä päivänä siitä päivästä, jona viimeinen allekirjoittajahallitus on tallettanut ratifioimis- tai hyväksymiskirjansa. Sopimuksen voimaantuloon saakka sopimuspuoli voi ilmoittaa ratifioimis- tai hyväksymiskirjansa tallettaessaan tai myöhemmin, että se katsoo sopimuksen sitovan sitä sen suhteissa muuhun sopimuspuoleen, joka on tehnyt samanlaisen ilmoituksen. Ilmoitukset tulevat voimaan kolmantenakymmenentenä päivänä siitä päivästä, jona ne on vastaanotettu. Esityksessä ehdotetaan, että Suomi jättäisi mainitun ilmoituksen. Sopimuksen voimaansaatamislaki on tarkoitettu tulemaan voimaan tasavallan presidentin asetuksella säädettävänä ajankohtana samaan aikaan kuin sopimus tulee voimaan.

## SISÄLLYS

ESITYKSEN PÄÄASIALLINEN SISÄLTÖ.....	1
SISÄLLYS.....	2
YLEISPERUSTELUT.....	3
1 JOHDANTO.....	3
2 NYKYTILA.....	4
2.1 Laki kansainvälisistä tietoturvaluusvelvoitteista.....	4
Lain yleinen soveltamisala.....	4
Lain suhde julkisuuslainsäädäntöön.....	4
Lain soveltaminen elinkeinonharjoittajiin.....	4
Lain täytäntöönpanoviranomaiset.....	5
Tietojen salassapito ja käytön sääntely.....	6
Turvallisuuksluokittelu ja -toimenpiteet.....	6
Henkilöturvallisuus.....	6
Yhteisöturvallisuus selvitys.....	7
2.2 Turvallisuuksluokitteluja koskeva lainsäädäntö.....	7
3 ESITYKSEN TAVOITTEET.....	8
4 ESITYKSEN VAIKUTUKSET.....	8
4.1 Vaikutukset kansalaisyiin.....	8
4.2 Vaikutukset elinkeinoelämään.....	9
4.3 Taloudelliset vaikutukset.....	9
4.4 Vaikutukset hallintoon.....	9
5 ASIAN VALMISTELU.....	9
YKSITYISKOHTAISET PERUSTELUT.....	10
1 Sopimuksen sisältö ja suhde Suomen lainsäädäntöön.....	10
2 Lakiehdotuksen perustelut.....	16
3 Voimaantulo.....	16
4 Eduskunnan suostumuksen tarpeellisuus ja käsittelyjärjestys.....	16
4.1 Eduskunnan suostumuksen tarpeellisuus.....	16
4.2 Käsittelyjärjestys.....	18
LAKIEHDOTUS.....	20
Tanskan, Suomen, Islannin, Norjan ja Ruotsin välillä tehdyn yleisen turvallisuuksluokitteluksen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta.....	20
SOPIMUSTEKSTI.....	21

## YLEISPERUSTELUT

### 1 Johdanto

Tietoturvallisuudella tarkoitetaan yleisesti ottaen kaikkia sellaisia menettelyjä, joiden avulla turvataan informaation sisällön suojaaminen ulkopuolisilta (tiedon luottamuksellisuus), tiedon muuttumattomuus (tiedon eheys) sekä tiedon käytettävyys. Tietoturvallisuuden varmistamiseksi käytetään erilaisia keinoja, joista tavallisimmat ovat henkilöstön luotettavuuden ja toimitilojen turvallisuuden varmistaminen, salassapitosäännökset ja tietojen käytön rajoittaminen vain soviittuun tarkoitukseen sekä erilaiset tietojen käsittelyyn ja siirtoon liittyvät menettelytapavaatimukset. Tietoturvallisuusvaatimukset kattavat informaation koko elinkaaren, toisin sanoen tietojen hankkimisen, muokkaamisen, käytön, luovutuksen, arkistoinnin ja hävittämisen.

Kansainväliseen yhteistyöhön liittyviin asiakirjoihin sisältyy salassa pidettäviä tietoja, joiden luvaton paljastuminen voi aiheuttaa merkittävää ja laajalle ulottuvaa vahinkoa keskeisille yleisille eduille. Tällaisten aineistojen asianmukaisesta käsittelystä on sen vuoksi pidettävä erityistä huolta. Kysymys on Suomen luotettavuudesta kansainvälisen yhteistyön osapuolena.

Kansainvälinen tietoturvallisuusyhteistyö, johon Suomikin osallistuu, käsittää perinteisesti diplomaattiseen toimintaan samoin kuin puolustus- ja poliisihallintojen väliseen yhteistyöhön liittyvän ei-julkisen tiedonvaihdon suojaamisen. Välittömän valtiovastuun piiriin kuuluvien kysymysten lisäksi kansainvälisillä tietoturvallisuusvelvoitteilla on kasvava merkitys myös taloudellisen, teollisen ja teknologisen yhteistyön kannalta. Yhä useampiin yritystason hankkeisiin liittyy turvallisuussuojatun tiedon hyödyntämistä. Näin on etenkin silloin, kun kyse on sellaisesta viranomaisen hankinnasta, jossa valtion suojattuja tietoja on annettava yritykselle kaupallisen sopimuksen toteuttamista varten. Tällaisia ovat perinteisesti olleet erityisesti puolustusalan hankinnat, mutta sektori on laajenemassa.

Pyrkimyksistä huolimatta ei ole osoittautunut mahdolliseksi toteuttaa tietoturvallisuusalan monenkeskistä yleissopimusta. Pääasiallinen syy tähän on kansallisten lainsäädäntöjen ja hallintorakenteiden ja -tapojen eroavaisuudet, jotka puolestaan heijastelevat tietoturvallisuuden sensitiivisyyttä osana kansallista kokonaisturvallisuutta.

Yleissopimuksen puuttuminen on siten pakkottanut valtiot, Suomi mukaan luettuna, etsimään kahdenvälisiä sopimusratkaisuja. Suomi on tehnyt ensimmäisen kahdenvälisen tietoturvallisuussopimuksensa Saksan liittotasavallan kanssa vuonna 2004. Sopimus tuli voimaan 16 päivänä heinäkuuta 2004 (SopS 96 ja 97/2004). Vuotta myöhemmin allekirjoitettiin Suomen ja Ranskan välinen sopimus, joka puolestaan tuli voimaan 1 päivänä elokuuta 2005 (SopS 66 ja 67/2005). Kumpikin suuri Euroopan unionin (EU) jäsenvaltio on Suomelle tärkeä yhteistyökumppani niin turvallisuushallinnon kuin taloudellisen vuoroaikatuksenkin aloilla.

Tietoturvallisuustarpeiden painottumista enenevässä määrin myös taloudelliseen toimintaan ilmentää Suomen ja Euroopan Avaruusjärjestön (ESA) välinen yhteistyösopimus, jäljempänä ESA:n tietoturvallisuussopimus, niin ikään vuodelta 2004 (SopS 94 ja 95/2004). Sopimuksen eräs keskeinen tavoite on turvata Suomen elinkeinoelämän mahdollisuudet osallistua tasavertaisesti muiden jäsenvaltioiden kanssa ESA:n turvallisuusluokiteltuihin tarjouskilpailuihin. Tietoturvallisuussopimus on tehty myös Länsi-Euroopan unionin (WEU) kanssa (SopS 41 ja 42/1998) ja Eurooppalaisen puolustusmateriaaliyhteistyöjärjestön (OCCAR) kanssa (SopS 109 ja 110/2008).

Mainittujen sopimusten lisäksi Suomi on tehnyt voimassaolevan tietoturvallisuussopimuksen Slovakian (SopS 116 ja 117/2007), Viron (SopS 12 ja 13/2008), Italian (SopS 23 ja 24/2008), Latvian (SopS 33 ja 34/2008), Puolan (SopS 46 ja 47/2008), Bulgarian (SopS 116 ja 117/2008), Slovenian (SopS 22 ja 23/2009), Tšekin (SopS 53 ja 54/2009) ja Espanjan (SopS 38 ja 39/2010) kanssa. Alle-

kirjoittamista odottaa sopimus Alankomaiden kanssa. Vireillä on lisäksi neuvottelut tietoturvaluusussopimuksesta Ison-Britannian, Luxemburgin ja Sveitsin kanssa. Myös EU:n jäsenvaltioiden välillä on vireillä hanke turvallisuusluokitellun tiedon suojaamista koskevaksi sopimukseksi.

Tanskan, Suomen, Islannin, Norjan ja Ruotsin välinen yleinen turvallisuus sopimus allekirjoitettiin Osllossa 7 päivänä toukokuuta 2010.

## 2 Nykytila

### 2.1 Laki kansainvälisistä tietoturvaluusvelvoitteista

#### *Lain yleinen soveltamisala*

Laki kansainvälisistä tietoturvaluusvelvoitteista (588/2004) säädettiin osana Suomen ja Saksan välisen tietoturvaluus sopimuksen sekä ESA:n tietoturvaluus sopimuksen voimaansattamista. Laki katsottiin tarpeelliseksi muun ohella sen vuoksi, että kansainvälisten sopimusten täytäntöön pamenteksi on tarve poiketa asiakirjajulkisuuteen ja -turvaluusuteen perustuvista kansallisista järjestelyistä, jotka perustuvat pääosin viranomaisten toiminnan julkisuudesta annettuun lakiin (621/1999), jäljempänä julkisuuslaki.

Lakia kansainvälisistä tietoturvaluusvelvoitteista sovelletaan erityissuojattaviin tietoineistoihin. Näillä tarkoitetaan salassa pidettäviä asiakirjoja ja materiaaleja sekä niihin sisältyviä tietoja, jotka on kansainvälisen turvallisuusvelvoitteen mukaisesti turvallisuusluokiteltu. Erityissuojattavaa tietoa ovat näin ollen Suomen viranomaiselle toimitetut asiakirjat ja niihin sisältyvät tiedot, joihin lähettäjä on kansainvälisen, Suomea sitovan sopimuksen tai muun kansainvälisen velvoitteen mukaisesti tehnyt turvallisuusluokkaa koskevan merkinnän. Lakia voidaan soveltaa vain, jos kansainvälinen sopimus on saatettu Suomessa voimaan perustuslaissa säädetyllä tavalla tai jos kysymys on Suomea muutoin sitovasta kansainvälisestä velvoitteesta.

Lain soveltamisalan piiriin kuuluvia erityissuojattavia tietoa ovat lisäksi

Suomen viranomaisen tai lain soveltamisalan piiriin kuuluvan elinkeinonharjoittajan laatimat asiakirjat, joista ilmenee Suomeen toimitettuihin asiakirjoihin sisältyviä tai materiaalista saatavissa olevia tietoja. Lain soveltamisalan piiriin kuuluvat niin ikään asiakirjat ja materiaalit, jotka on Suomessa tuotettu salassa pidettävän turvallisuusluokitellun tiedon perusteella.

Laissa säädetyt turvallisuusvelvoitteita sovelletaan silloinkin, kun sopimus tai säädös, johon säännösten soveltaminen perustuu, ei enää ole voimassa (15 §). Soveltaminen jatkuu niin kauan kuin se turvallisuusluokituksen perusteena olevan yleisen edun vuoksi on tarpeen.

#### *Lain suhde julkisuuslainsäädäntöön*

Kansainvälisistä tietoturvaluusvelvoitteista annettuun lakiin sisältyy useita kansallisten asiakirjojen tietoturvaluudesta annetuista säännöksistä poikkeavia säännöksiä. Laissa on kuitenkin yleinen viittaussäännös julkisuuslakiin. Niitä osin kuin suomalaisten viranomaisten asiakirjoihin sisältyy muita kuin kansainvälisten tietoturvaluusvelvoitteiden piiriin kuuluvia tietoja kansainvälisestä yhteistyöstä, on sovellettava julkisuuslain ja sen nojalla annettuja säännöksiä. Laissa on myös erityissäännös, joka koskee päätöksentekovaltaa siinä tilanteessa, jossa tietoja pyydetään julkisuuslain nojalla erityissuojattavasta aineistosta. Julkisuuslain mukaan tiedonsaantia koskevan pyynnön voi käsitellä ja ratkaista se viranomainen, jonka hallussa asiakirja on. Tiedonsaantipyyntö voidaan kuitenkin siirtää toisen viranomaisen ratkaistavaksi julkisuuslain 15 §:ssä säädetyissä tilanteissa.

#### *Lain soveltaminen elinkeinonharjoittajiin*

Lakia sovelletaan viranomaisten lisäksi myös elinkeinonharjoittajaan ja tämän palveluksessa olevaan silloin, kun elinkeinonharjoittaja on sopimusosapuolena turvallisuusluokitellussa sopimuksessa tai osallistuu tällaista sopimusta edeltävään hankintakilpailuun tai toimii tällaisen elinkeinonharjoittajan alihankkijana (1 § 2 mom.).

Turvaluusluokitellulla sopimuksella tarkoitetaan sopimusta, jonka toisen valtion vi-

ranomainen tai siinä kotipaikkaansa pitävä yritys taikka kansainvälinen järjestö tai toimitielin aikoo tehdä tai on tehnyt kansainvälisessä tietoturvaluusvelvoitteessa tarkoitulla tavalla Suomessa kotipaikkaansa pitävän elinkeinonharjoittajan kanssa, jos tarjouskilpailuun osallistuminen tai sopimuksen toteuttaminen voi edellyttää pääsyä erityis-suojattavaan tietoaineistoon (2 § 3 kohta).

Lain mukaan elinkeinonharjoittaja voi pyytää yhteisöturvaluusvelvoitteen ja arvion tekemistä voidakseen osallistua toisen valtion viranomaisen tai siinä kotipaikkaansa pitävän yrityksen järjestämään tarjouskilpailuun riippumatta siitä, onko Suomi tehnyt kyseisen valtion kanssa sopimuksen, jossa on määräksiä tietoturvaluusvelvoitteista (1 § 3 mom.). Säännöksen tarkoituksena on turvata suomalaisten yritysten kilpailumahdollisuudet hankinnoissa silloinkin, kun hankintaan sovellettavissa olevaa kansainvälistä tietoturvaluusvelvoitetta ei ole. Useimmat valtiot kuitenkin edellyttävät kahdenvälisen tietoturvaluusvelvoitteen olemassa oloa ulkomaisen turvaluusvelvoitteen hyväksymiseksi.

Elinkeinonharjoittajalla ja tämän palveluksessa tai toimeksiannosta toimivalla on erityis-suojattavia tietoaineistoja koskeva salassapitovelvollisuus (6 ja 7 §). Elinkeinonharjoittajalla on myös velvollisuus kansainvälisten tietoturvaluusvelvoitteiden toteuttamiseksi antaa tietoja sekä sallia viranomaisen ja kansainvälisen toimielimen tai sopimusvaltion edustajan tutustuminen turvaluusjärjestelyihinsä ja toimitiloihinsa (16 § 2 mom., 18 § 2 mom.).

#### *Lain täytäntöönpanoviranomaiset*

Laissa on säännökset (4 §) niistä viranomaisista, jotka huolehtivat kansainvälisten tietoturvaluusvelvoitteiden hoitamisesta. Kansallisena turvaluusviranomaisena (National Security Authority, NSA) kansainvälisten tietoturvaluusvelvoitteiden toteuttamiseen liittyvissä tehtävissä toimii ulkoasiainministeriö. Puolustusministeriö, pääesikunta, suojelupoliisi ja Viestintävirasto toimivat määrättyinä turvaluusviranomaisina (Designated Security Authority, DSA). Näille viranomaisille voi kuulua muun ohella

tarjous- ja hankintamenettelyihin liittyvien asiakirjojen turvaluusluokittelu.

Henkilöturvaluusvelvoitteen liittyvien turvaluusvelvoitteiden laadinnasta huolehtivat suojelupoliisi ja pääesikunta (11 §). Yhteisöturvaluusvelvoitteen laadinta kuuluu lain mukaan suojelupoliisille, paitsi silloin, kun kyse on puolustukseen liittyvästä hankinnasta, jolloin selvitysten tekemisestä huolehtii pääesikunta (12 §). Kansainvälisistä tietoturvaluusvelvoitteista annetun lain 5 § 2 momentin mukaan kansallinen turvaluusviranomaisen ja tehtävään määrätty turvaluusviranomaiset voivat sen estämättä, mitä muun muassa toimivallasta yhteisöturvaluusvelvoitteiden laadinnasta säädetään, sopia tietyn tehtävän tai tehtäväkokonaisuuden hoitamisesta toisen turvaluusviranomaisen lukuun, jos järjestely on tarpeen tehtävien hoitamiseksi tarkoituksenmukaisesti, taloudellisesti ja joutuisasti.

Laissa ei aiemmin määritelty viranomaisista, jonka tehtävänä olisi arvioida tietojärjestelmien ja tietoliikennejärjestelyjen turvaluusvelvoitetta. Eduskunnan 1 päivänä lokakuuta 2010 hyväksymässä kansainvälisistä tietoturvaluusvelvoitteista annetun lain muuttamisesta annetun lain (8852010) 4 §:n 1 momentissa Viestintävirasto nimettiin määrättyksi turvaluusviranomaiseksi.

Laissa kansainvälisistä tietoturvaluusvelvoitteista on säännökset viranomaisia ja elinkeinonharjoittajaa koskevasta tiedonantovelvollisuudesta (16 §). Säännösten tarkoituksena on varmistaa, että toimivaltaiset turvaluusviranomaiset voisivat saada niille kuuluvien tehtävien hoitamiseksi tarpeelliset tiedot. Viranomaiset voivat myös salassapitovelvollisuuden estämättä antaa kansainväliseen tietoturvaluusvelvoitteeseen perustuvaa yhteistyötä varten salassa pidettäviä tietoja ulkomaiselle sopimuspuolelle (17 §). Viranomaisella on myös oikeus sallia kansainväliseen tietoturvaluusvelvoitteeseen perustuva kansainvälisen järjestön, toimielimen tai sopimusvaltion edustajan tutustuminen viranomaisen toteuttamiin turvaluusjärjestelyihin ja toimitiloihin riippumatta siitä, mitä turvaluusjärjestelyjen salassapidosta säädetään taikka säädetään tai määrätään pääsystä tiloihin, joissa käsitellään tai säilytetään salassa pidettäviä tietoja (18 §).

Kansallisen turvallisuusviranomaisen on lain mukaan ilmoitettava kansainvälisessä tietoturvallisuusveloitteessa tarkoitetuissa tapauksissa toiselle sopimuspuolelle tietoonsa tulleesta turvallisuusluokiteltujen tietojen suojan vaarantumisesta ja tietoturvallisuutta koskevan määräyksen loukkaamisesta sekä ryhdyttävä toimenpiteisiin asian selvittämiseksi samoin kuin rangaistavaan tekoon syylistyneen syytteeseen saattamiseksi (19 §).

#### *Tietojen salassapito ja käytön sääntely*

Aiemmin laki kansainvälisistä tietoturvallisuusveloitteista lähti siitä, että erityissuojattava tietoaineisto on pidettävä salassa (6 § 1 mom.). Salassapitovelvollisuus koskee myös elinkeinonharjoittajaa tämän ollessa hankeosapuolena turvallisuusluokitellussa sopimuksessa.

Suomen tekemissä, käytännössä kahdenvälisissä sopimuksissa, jotka koskevat eri maiden viranomaisten välistä salassapidettävien tietojen vaihtoa, on säännönmukaisesti määräys, joka rajoittaa luovutettujen tietojen käyttöä. Tämän mukaisesti erityissuojattavaa tietoaineistoa saa käyttää ja luovuttaa vain siihen tarkoitukseen, jota varten se on annettu, jollei se, joka on määritellyt aineiston turvallisuusluokan, ole antanut muuhun suostumustaan (6 § 2 mom.). Erityissuojattavien tietoaineistojen käyttöä koskee siten vahva käyttötarkoitussidonnaisuus.

Kansainvälisistä tietoturvallisuusveloitteista annetun lain 6 §:n 1 momenttia muutettiin lokakuussa 2010 siten, että tiedon salassapito on riippuvainen kunkin sopimuksen tai kansainvälisen veloitteen sisällöstä (HE 53/2010 vp – EV 135/2010 vp.). Lainmuutos oli edellytyksenä muun muassa kyseessä olevan Pohjoismaiden välisen yleisen turvallisuus sopimuksen hyväksymiselle ja voimaansaattamiselle Suomessa, koska sopimus ei edellytä tiedon ehdotonta salassapitoa. Muutos on tullut voimaan 1 päivänä marraskuuta 2010.

#### *Turvallisuusluokittelu ja -toimenpiteet*

Laissa säädetään velvollisuudesta merkitä erityissuojattavaan tietoaineistoon sen turvallisuusluokka. Tietoaineistoon tehty merkintä turvallisuusluokasta osoittaa minkälaisia

toimenpiteitä aineistoa käsiteltäessä on noudatettava (8 §). Mitä korkeampaan turvallisuusluokkaan aineisto kuuluu, sitä tiukempia tietoturvallisuustoimenpiteitä edellytetään. Laissa on yleinen velvoite toteuttaa tietoaineiston käsittelyssä sen turvallisuusluokkaa koskevia käsittelymääräyksiä sekä valtuus säätää erityissuojattavan tietoaineiston käsittelyssä noudatettavista turvallisuusluokitusta vastaavista teknisistä turvallisuustoimenpiteistä valtioneuvoston asetuksella (9 §). Tietoturvallisuudesta valtionhallinnossa annetun valtioneuvoston asetuksen (681/2010), jäljempänä tietoturvallisuusasetus, 11 §:ssä on säädetty turvallisuusluokitusmerkintää koskevista erityissäännöksistä ja 12 §:ssä turvallisuusluokituksen vastaavuudesta.

Turvallisuusluokiteltuja aineistoja käsiteltäessä on lain mukaan huolehdittava siitä, että tietoja säilytetään asianmukaisissa tiloissa. Tilojen turvallisuusvaatimuksista on säädetty tietoturvallisuusasetuksen 14 §:ssä.

Lakiin kansainvälisistä tietoturvallisuusveloitteista on kirjattu kansainvälisissä sopimuksissa yleinen vaatimus siitä, että turvallisuusluokiteltuja tietoja viranomaisissa käsiteltäessä noudatetaan suurta pidättyvyyttä ja että tietoihin annetaan pääsy vain niille, jotka tarvitsevat tietoja tehtäviensä hoitamisessa. Nämä henkilöt on nimettävä etukäteen, jos sopimuksessa tätä edellytetään. Sama koskee myös 1 §:n 2 momentissa tarkoitettua elinkeinonharjoittajaa (6 § 3 mom.).

#### *Henkilöturvallisuus*

Kansainvälisessä tietoturvallisuusveloitteessa edellytetty henkilöturvallisuutta koskeva turvallisuus selvitys tehdään siten kuin turvallisuus selvityksistä annetussa laissa (177/2002) ja sen nojalla säädetään. Siten esimerkiksi selvityksen kohteena olevan henkilön oikeudet määräytyvät sanotun lain mukaisesti.

Kansainvälisistä tietoturvallisuusveloitteista annetussa laissa on kuitenkin kaksi säännöstä, jotka ovat erityissäännöksiä suhteessa turvallisuus selvityksistä annettuun lakiin. Suppea turvallisuus selvitys on mahdollista laatia muissakin kuin turvallisuus selvityksistä annetun lain 19 §:ssä luetelluissa tapauksissa, jos se on tarpeen kansainvälisen tietoturvallisuusveloitteen toteuttamiseksi

(11 § 1 mom.). Toinen erityissäännös koskee viranomaisten toimivaltaa. Turvallisuusselvityksen tekee pääesikunta silloin, kun turvallisuusselvityksen laatiminen on tarpeen puolustushallintoa tai puolustushankintoja koskevan kansainvälisen velvoitteen toteuttamiseksi. Muissa tapauksissa henkilöön liittyvien turvallisuusselvitysten laadinnasta huolehtii suojelupoliisi (11 § 2 mom.). Turvallisuusselvityksistä annetun lain 10 §:n 2 momentin mukaan turvallisuusselvitykseen ei saa sisällyttää selvityksen laatineen viranomaisen arviota selvityksen kohteena olevan henkilön luotettavuudesta tai sopivuudesta virkaan tai tehtävään, ellei lain 9 §:ssä tarkoitettu valtiosopimus tai muu kansainvälinen velvoite tätä edellytä. Koska pääsääntönä on, että turvallisuusselvitys ei sisällä arviota henkilön luotettavuudesta, laissa kansainvälisistä tietoturvallisuusvelvoitteista on erikseen mainittu henkilön luotettavuuden arviointi. Tällaisen arvion tekee turvallisuusselvityksen perusteella kansallinen turvallisuusviranomaisen tai, jos turvallisuusviranomaisen välillä on niin sovittu, tehtävään määrätty turvallisuusviranomaisen (11 § 3 mom.).

Arvioinnin perusteella annetaan henkilöturvallisuutta koskeva todistus (Personal Security Clearance Certificate). Se toimitetaan tavanomaisesti sopimuspuolen turvallisuusviranomaiselle sopimuksen osoittamalla tavalla. Laissa kansainvälisistä tietoturvallisuusvelvoitteista on myös säännökset todistuksen antamisesta henkilölle itselleen (14 §).

### *Yhteisöturvallisuusselvitys*

Yhteisöturvallisuusselvityksellä varmistetaan elinkeinonharjoittajan toimitilojen ja käsittelykäytäntöjen asianmukaisuus sekä henkilöstön osaaminen. Elinkeinonharjoittajan luotettavuuden arvioinnilla varmistetaan erityisesti siitä, kuinka hyvin tämä pystyy huolehtimaan turvallisuusluokiteltujen tietojen suojaamisesta. Yhteisöturvallisuusmenettely ja siihen perustuva arvio toteutetaan pääosin elinkeinonharjoittajalta itseltään saatujen tietojen perusteella sekä tämän toimitilojen turvallisuuden kartoituksella, ja tarvittavista toimenpiteistä huolehditaan elinkeinonharjoittajan kanssa tehtävän sopimuksen avulla. Selvityksen laatii puolustushallinnon alaan kuuluvissa asioissa pääesikunta ja muulloin

suojelupoliisi. Selvitystä laadittaessa on otettava huomioon kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa yksilöidyt seikat, muun muassa se, miten suojataan turvallisuusluokiteltuja tietoja oikeudettomalta ilmitulolta, muuttamiselta ja hävittämislä, ja miten estetään asiaton pääsy tiloihin, joissa turvallisuusluokiteltuja tietoja käsitellään tai joissa harjoitetaan turvallisuusluokitellussa sopimuksessa tarkoitettua toimintaa (12 §).

Pääesikunta voi tehdä lain soveltamisalan piiriin kuuluvan elinkeinonharjoittajan kanssa sopimuksen, jossa elinkeinonharjoittaja sitoutuu toimenpiteisiin kansainvälisten tietoturvallisuusvelvoitteiden toteuttamiseksi (13 §). Sopimuksessa voidaan yksityiskohtaisemmin määrittellä ne toimenpiteet, jotka elinkeinonharjoittaja toteuttaa täyttääkseen kansainvälisistä tietoturvallisuusvelvoitteista johtuvat vaatimukset. Sopimuksessa elinkeinonharjoittaja sitoutuu myös tekemään ne mahdolliset tarkistukset toimintaansa, jotka toiminnan turvallisuuskartoituksessa on havaittu. Turvallisuusselvityksen ja mahdollisen sopimuksen jälkeen pääesikunta voi tehdä arvion elinkeinonharjoittajan luotettavuudesta ja antaa tätä koskevan turvallisuustodistuksen (Facility Security Clearance Certificate). Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 13 §:n muutosesityksen johdosta vastaava sitoutumismenettely tulee toteutumaan myös suojelupoliisin suorittamissa yhteisöturvallisuusselvityksissä.

### **2.2 Turvallisuusselvityksiä koskeva lainsäädäntö**

Henkilöstöturvallisuuteen liittyvistä turvallisuusselvityksistä säädetään turvallisuusselvityksistä annetussa laissa. Lain tarkoituksena on turvallisuusselvitysmenettelyä käyttämällä parantaa mahdollisuuksia ennakolta estää rikokset, jotka vakavasti vahingoittaisivat keskeisiä yleisiä tai yksityisiä etuja taikka erittäin merkittävää tietoturvallisuutta.

Turvallisuusselvitys voidaan tehdä virkaan tai tehtävään hakeutuvasta, tehtävään tai koulutukseen otettavasta taikka virkaa tai tehtävää hoitavasta henkilöstä, ja se voi olla perusmuotoinen, laaja tai suppea. Turvallisuusselvitys tehdään laissa määritellyissä tapauksissa, kuten silloin, kun Suomea sitova val-

tiosopimus tai muu kansainvälinen velvoite edellyttää turvallisuus selvityksen tekemistä tai sen perusteella laaditun todistuksen esittämistä.

Yksityisyyden suojan perusoikeusluonteen vuoksi turvallisuus selvitysmenettely on tarkan muotosidonnaista. Turvallisuus selvitys voidaan tehdä vain selvityksen kohteena olevan henkilön etukäteen antaman, nimenomaisen ja kirjallisen suostumuksen perusteella. Myös turvallisuus selvitysmenettelyssä käytettävät rekisterit on laissa lueteltu tyhjentävästi.

Jokaisella on oikeus saada tieto siitä, onko hänestä tehty turvallisuus selvitys tiettyä tehtävää varten. Selvityksen kohteella on myös oikeus pyynnöstä saada toimivaltaiselta viranomaiselta perusmuotoisen tai laajan turvallisuus selvityksen tiedot. Tiedonsaantioikeus ei kuitenkaan koske sellaisesta rekisteristä peräisin olevaa tietoa, johon rekisteröidyllä ei ole tarkastusoikeutta.

Turvallisuus selvityslain kokonaistarkistusta varten on asetettu oikeusministeriön työryhmä. Työryhmälle annettuun tehtävään kuuluu turvallisuus selvityslain kehittäminen siten, että se vastaa Suomea sitovia velvoitteita ja kansainvälisesti yleisesti sovellettavia käytäntöjä. Työryhmän tavoitteena on antaa hallituksen esitys asiasta vuonna 2011.

### 3 Esityksen tavoitteet

Esityksen tavoitteena on saattaa voimaan Tanskan, Suomen, Islannin, Norjan ja Ruotsin välinen tietoturvaluus sopimus ja sillä tavoin parantaa Pohjoismaiden välistä yhteistyötä sekä turvata suomalaisten yritysten mahdollisuudet osallistua sellaisiin kansainvälisiin sekä Suomen ja muiden Pohjoismaiden välisiin hankkeisiin, joiden toteuttaminen saattaa edellyttää erityissuojattavien tietojen vaihtoa.

### 4 Esityksen vaikutukset

#### 4.1 Vaikutukset kansalaisiin

Sopimuksen voimaansaattamisen myötä muista Pohjoismaista Suomeen toimitettuihin turvallisuus luokiteltuihin tietoihin ja materiaaleihin sovellettaisiin lakia kansainvälisistä tietoturvaluus velvoitteista. Lakiin sisältyy

erityissäännös, jonka mukaan toisen sopimuspuolen salassa pidettävät ja turvallisuus luokitellut asiakirjat ja niihin sisältyvät tiedot ovat myös Suomessa salassa pidettäviä. Säännös poikkeaa muodoltaan julkisuus lain yleistä etua koskevista salassapitosäännöksistä, joissa salassapito on useimmissa tapauksissa riippuvainen siitä, minkälaisia vaikutuksia tietojen antamisella olisi suojattavalle edulle. Kansainvälisistä tietoturvaluus velvoitteista annetun lain mukainen salassapito on näin ollen sanamuodon mukaan kattavampi kuin yleisessä julkisuus laissa. Lain 6 §:ää on kuitenkin muutettu 1. päivänä marraskuuta 2010 voimaantulleella lailla siten, että jatkossa erityissuojattava tietoaineisto on pidettävä salassa, jollei kansainvälisestä tietoturvaluus velvoitteesta muuta johdu. Pohjoismaiden välisessä sopimuksessa on kysymys asiakirjoista, joita jokin sopimuspuoli pitää salassa pidettävänä ja jotka se on määritellyt ja merkinnyt korkean tietoturvaluus tasoa edellyttäväksi. Tällaisia asiakirjoja on säännönmukaisesti pidettävä salaisina myös julkisuus lain 24 §:n 1 momentin 2 kohdan mukaan. Merkittävimpänä erona on se, että viranomaisella ei olisi kansainvälisessä tietoturvaluus velvoitteesta tarkoitettuun asiakirjaan kohdistuvaa tiedonsaantipyntöä ratkaistessaan velvollisuutta erikseen perustella tiedon antamisesta aiheutuvaa vahinkoa. Tiedonsaantipyntö olisi muutoin käsiteltävä julkisuus lain mukaisesti. Jos luokituksen oikeellisuudesta tai siitä, minkä asiakirjan tietojen vuoksi luokitusmerkintä on tehty, syntyy epäselvyyttä, viranomaisen on otettava yhteyttä asiakirjan laatineeseen sopimuspuoleen.

Edellä olevan perusteella voidaan arvioida, että Pohjoismaiden välisen tietoturvaluus sopimuksen voimaansaattamista koskeva lakiehdotus ei asiallisesti vaikuta kansalaisten tiedonsaantia vähentävästi suhteessa siihen, mitä tiedonsaanti yleisen lainsäädännön mukaan on.

Henkilöstöturvallisuus on keskeinen tietoturvaluus uuden osa-alue. Koska jo laki kansainvälisistä tietoturvaluus velvoitteista edellyttää turvallisuus selvityksistä annetun lain mukaisen menettelyn käyttämistä henkilöstön luotettavuuden varmistamisessa, ehdotetun voimaansaattamislain hyväksyminen ei merkitisi kansalaisten yksityiselämän ja henkilötie-



tojen suojan kaventumista aikaisempaan verrattuna.

#### **4.2 Vaikutukset elinkeinoelämään**

Sopimus antaa suomalaiselle teollisuudelle mahdollisuuden saada sellaisia tilauksia tai osallistua sellaisiin hankkeisiin, joiden toteuttaminen edellyttää pääsyä Pohjoismaiden turvallisuusluokiteltuihin tietoihin. Vastavasti sopimus antaa muiden Pohjoismaiden teollisuudelle mahdollisuuden saada sellaisia tilauksia tai osallistua sellaisiin hankkeisiin, joiden toteuttaminen edellyttää pääsyä Suomen turvallisuusluokiteltuun tietoon.

#### **4.3 Taloudelliset vaikutukset**

Esityksellä ei ole vaikutusta valtion talousarvioon eikä muitakaan vähäistä merkittävämpiä taloudellisia vaikutuksia.

#### **4.4 Vaikutukset hallintoon**

Esitykseen sisältyvän sopimuksen ja lain hyväksymisestä ei aiheudu hallintoa koskevia muutosvelvoitteita tai -tarpeita.

### **5 Asian valmistelu**

Valtioneuvoston yleisistunto päätti neuvotteluvaltuuskunnan asettamisesta 26 päivänä toukokuuta 2005. Suomen neuvotteluvaltuuskuntaan kuului jäsenenä oikeusministeriön, kauppaja teollisuusministeriön, puolustusministeriön sekä ulkoasiainministeriön edustajia.

Sopimusneuvottelut alkoivat neuvotteluvaltuuskunnan asettamisen jälkeen Norjan vetäminä kesällä 2005 ja sopimus neuvoteltiin vuoden 2005 aikana pitkälti valmiiksi. Sopimuksen viimeistelyä hidasti kuitenkin Tanskan haluttomuus edetä, koska Tanskan viranomaiset eivät nähneet sopimukselle suurta tarvetta. Suomi ja Ruotsi ajoivat voimakkaasti sopimusneuvottelujen jatkamista, koska sopimuksella on merkitystä erityisesti maiden puolustushallinnoille.

Syksyllä 2008 neuvotteluja jatkettiin Osllossa. Neuvottelujen aikana sopimusta uudistettiin ja yksinkertaistettiin vastaamaan uusimpia tietoturvallisuusvaatimuksia. Suomalainen oli neuvotteluissa aktiivinen rooli oman mallisopimuksensa ansiosta. Sopimus saatiin valmiiksi ja se jäi odottamaan Tanskan suostumusta allekirjoitukselle. Kuluvan vuoden alussa Tanska ilmoitti, että se on valmis sopimuksen allekirjoittamiseen, ja sopimus allekirjoitettiin 7 päivänä toukokuuta 2010 Osllossa. Hallituksen esitys on valmisteltu virkautyönä ulkoasiainministeriössä. Sopimuksen valmisteluun ja sen neuvotteluun on osallistunut edustajia ulkoasiainministeriöstä, oikeusministeriöstä, puolustusministeriöstä sekä työ- ja elinkeinoministeriöstä.

Esityksestä on pyydetty lausunnot oikeusministeriöltä, työ- ja elinkeinoministeriöltä, puolustusministeriöltä, valtiovarainministeriöltä, sisäasiainministeriöltä, liikenne- ja viestintäministeriöltä, suojelupoliisilta, pääesikunnalta, Viestintävirastolta sekä Elinkeinoelämän keskusliitolta (EK). Lausunnot on otettu huomioon esitystä viimeisteltäessä.

## YKSITYISKOHTAISET PERUSTELUT

### 1 Sopimuksen sisältö ja suhde Suomen lainsäädäntöön

*1 artikla. Tarkoitus ja soveltamisala.* Artiklan 1 kappaleessa määritellään sopimuksen tarkoituksiksi suojata kahden Pohjoismaan kesken vaihdettu tai sopimuspuolten lainkäyttövaltaan kuuluvien hankeosapuolten vaihtama turvallisuusluokiteltu tieto. Artiklassa määritellään myös ne toiminnot, joihin sopimusta sovelletaan. Näitä ovat ulko-, puolustus-, turvallisuus- tai poliisiasiat sekä tiede-, elinkeino- ja teknologiayhteistyöasiat. Rajaturvallisuuden ylläpitämisen katsotaan sisältyvän edellä mainittuihin aloihin. Sopimusta sovelletaan myös sellaisen tiedon välittämiseen, joka syntyy tai jota tuotetaan vaihdettavan tiedon perusteella. Artiklan 2 kappaleen mukaan sopimuspuoli ei voi vedota sopimukseen saadakseen turvallisuusluokiteltua tietoa, jota muut sopimuspuolet ovat saaneet kolmannelta sopimuspuolelta.

*2 artikla. Määritelmät.* Artiklassa määritellään sopimuksen soveltamisen kannalta keskeiset käsitteet.

Turvallisuusluokitellulla tiedolla tarkoitetaan missä tahansa muodossa olevaa tietoa, joka jonkin sopimuspuolen lainsäädännön mukaan on suojattava katoamiselta, luvattomalta ilmaisemiselta tai muulta vaarantumiselta, ja joka on merkitty turvallisuusluokituksi. Määritelmä kattaa myös turvallisuusluokitellun tiedon pohjalta tuotetun tiedon, asiakirjan tai muun aineiston. Kohta on sopusoinnussa kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 2 §:n 2 kohdan kanssa.

Lähettävällä sopimuspuolella tarkoitetaan sopimuspuolta tai sen lainkäyttövaltaan kuuluvaa muuta valtion viranomaista tai julkistai yksityisoikeudellista oikeushenkilöä, joka välittää turvallisuusluokiteltua tietoa. Vastanottavalla sopimuspuolella tarkoitetaan sopimuspuolta tai muuta sen lainkäyttövaltaan kuuluvan valtion viranomaista tai julkistai yksityisoikeudellista oikeushenkilöä, jolle lähettävä sopimuspuoli välittää turvallisuusluokiteltua tietoa.

Turvallisuusluokitellulla sopimuksella tarkoitetaan sopimusta, johon sisältyy tai liittyy

turvallisuusluokiteltua tietoa. Kohta on sopusoinnussa kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 2 §:n 3 kohdan kanssa.

Toimivaltaisella turvallisuusviranomaisella tarkoitetaan turvallisuusasioista vastaavaa hallituksen viranomaista. Suomessa mainittuna viranomaisena toimii kansainvälisistä tietoturvallisuusvelvoitteista annetun lain mukaan ulkoasiainministeriö, missä tehtävää hoitaa Kansallinen turvallisuusviranomainen. Tämän lisäksi puolustusministeriö, suojelupoliisi, pääesikunta ja Viestintävirasto toimivat määrättyinä turvallisuusviranomaisina.

Hankeosapuolella tarkoitetaan luonnollista henkilöä tai oikeushenkilöä, joka on oikeustoimikelpoinen tekemään sopimuksia.

Tietoturvaloukkauksella tarkoitetaan kansallisten turvallisuusmääräysten vastaista tekoa tai laiminlyöntiä, jonka johdosta turvallisuusluokiteltu tieto saattaa vaarantua tai olla vaarassa paljastua.

Turvallisuusselvityksellä tarkoitetaan tutkintamenettelyyn perustuvaa myönteistä arviota siitä, että luonnolliselle henkilölle tai oikeushenkilölle voidaan sallia pääsy tiettyyn turvallisuusluokkaan kuuluvaan turvallisuusluokiteltuun tietoon sekä antaa oikeus käsitellä sitä asianomaisten kansallisten turvallisuusmääräysten mukaisesti. Suomessa suojelupoliisi ja pääesikunta huolehtivat henkilöiden taustojen selvittämisestä turvallisuusselvityksistä annetun lain nojalla.

Tiedonsaantitarpeella (need to know) tarkoitetaan periaatetta, jonka mukaan luonnollisille henkilöille voidaan sallia pääsy turvallisuusluokiteltuun tietoon ainoastaan heidän virkavelvollisuksiensa tai tehtäviensä yhteydessä. Vastaaventyypinen määritelmä sisältyy myös kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 6 §:n 3 momenttiin.

Kolmannella osapuolella tarkoitetaan toimielintä, kansainvälistä tai kansallista järjestöä, oikeushenkilöä tai valtiota, joka ei ole sopimuksen sopimuspuoli. Sopimuksen sopimuspuolta pidetään ”kolmantena osapuolena” yhteistyössä, johon kyseinen sopimuspuoli ei osallistu.

*3 artikla. Turvallisuusluokitellun tiedon suojaaminen.* Artiklan 1 kappaleessa asetetaan sopimuspuolille velvollisuus toteuttaa kansallisen lainsäädäntönsä mukaisesti asianmukaiset toimet suojatakseen sopimuksessa tarkoitetun turvallisuusluokitellun tiedon. Sopimuspuolet antavat kaikelle sopimuksessa tarkoitetulle turvallisuusluokitellulle tiedolle samantasoisien suojan, kuin omalle vastaavaan 5 artiklan mukaiseen turvallisuusluokkaan kuuluvalla tiedolle. Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 8 §:ssä velvoitetaan viranomaista merkitsemään turvallisuusluokka erityissuojattavaan tietoaineistoon. Tietoturvallisuusasetuksen 11 §:ssä on säädetty tarkemmin turvallisuusluokitusmerkinnöistä sekä 12 §:ssä niiden vastaavuudesta kansainvälisiä tietoturvallisuusvelvoitteita toteutettaessa.

Pääsy turvallisuusluokkaan CONFIDENTIAL tai sitä ylempään luokkaan kuuluvaan turvallisuusluokiteltuun tietoon, sekä paikkoihin ja tiloihin, joissa säilytetään turvallisuusluokiteltuun tietoon liittyvää toimintaa, sallitaan artiklan 2 kappaleen mukaisesti ainoastaan henkilöille, joista on tehty turvallisuusselvitys ja joilla on tiedonsaantitarve. Määräys vastaa kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 6 §:n 3 momentin ja tietoturvallisuusasetuksen 13 §:n säännöksiä sekä tilojen turvallisuuden osalta lain 10 §:n ja asetuksen 14 §:n säännöksiä.

Artiklan 3 kappaleen mukaan sopimuspuolet tunnustavat vastavuoroisesti toistensa tekemät turvallisuusselvitykset. Henkilöturvallisuusselvityksistä on säädetty turvallisuusselvityksistä annetussa laissa ja yhteisöturvallisuusselvityksistä kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 12 §:ssä.

Artiklan 4 kappaleen mukaan sopimuspuolet valvovat turvallisuuslainsäädännön, -määräysten ja -käytäntöjen noudattamista lainkäyttövaltaansa kuuluvissa virastoissa, toimistoissa ja tiloissa, joissa säilytetään, kehitetään, tuotetaan ja/tai käytetään toisten sopimuspuolten turvallisuusluokiteltua tietoa.

*4 artikla. Turvallisuusluokitellun tiedon ilmaiseminen ja käyttö.* Artiklan 1 kappale velvoittaa sopimuspuolet noudattamaan luovuttajan suostumuksen periaatetta perustuslakiansa sekä muiden kansallisten lakiansa ja määräystensä mukaisesti. Sopimuspuolet ei-

vät saa ilmaista sopimuksessa tarkoitettua turvallisuusluokiteltua tietoa kolmansille osapuolille tai muiden maiden kansalaisille sopimatta asiasta ensin kirjallisesti lähettävän sopimuspuolen kanssa. Sopimuspuolen toisille sopimuspuolille välittämää turvallisuusluokiteltua tietoa saa käyttää ainoastaan sille määrättyyn tarkoitukseen.

Kaikki valtiot eivät takaa sopimuksen perusteella tietojen ehdotonta salassapitoa, vaan asia jää kansalliseen lainsäädäntöön perustuvan tapauskohtaisen vahinkoedellytysharkinnan varaan. Esimerkiksi Ruotsissa kansallisen lainsäädännön (tryckfrihetsförordning SFS 1949:105) mukaan pääsääntönä on virallisten asiakirjojen – myös muista valtioista saatujen – julkisuus ja siitä voidaan poiketa ainoastaan, mikäli kansallinen turvallisuus tai Ruotsin suhteet ulkovaltoihin tai kansainvälisiin järjestöihin ovat vaarassa. Käytännössä Ruotsissa ei ole kuitenkaan koskaan toimittu vastoin vieraan valtion salassapitopyyntöä. Mikäli tällaista tietoa luovutettaisiin luvatta, voitaisiin sen katsoa vaarantavan Ruotsin suhteet kyseiseen valtioon, jolloin vahinkoedellytys täytyisi.

Edellä olevan johdosta katsottiin, että edellytyksenä pohjoismaisen tietoturvallisuus sopimuksen hyväksymiselle ja voimaansaattamiseksi Suomessa olisi kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 6 §:n 1 momentin muuttaminen (HE 53/2010 vp). Hallituksen esityksessä 6 §:n muutosta perusteltiin sillä, että Suomen käymissä tietoturvallisuus sopimusten neuvotteluissa on tullut esiin tilanteita, joissa toinen sopimuspuoli ei takaa sopimuksen perusteella ehdotonta salassapitoa, vaan joissa asia jää kansalliseen lainsäädäntöön perustuvan tapauskohtaisen vahinkoedellytysharkinnan varaan. Tarkoituksenmukaista ei näissä tilanteissa ole, että Suomi noudattaa laajempaa salassapitovelvollisuutta, kuin toiset sopimuspuolet. Tästä syystä esityksessä ehdotettiin, että kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 6 §:n 1 momenttiin otetaan lauseke, jonka mukaan salassapitovelvollisuus olisi riippuvainen kunkin sopimuksen tai muun kansainvälisen velvoitteen sisällöstä. Lakiehdotus hyväksyttiin eduskunnassa muuttumattomana ja se on tullut voimaan 1 päivänä marraskuuta 2010.

Kansainvälisistä tietoturvallisuusveloitteista annetun lain 6 § 2 momentissa säädetään siitä, että erityissuojattavaa tietoaineistoa saa käyttää ja luovuttaa vain siihen tarkoitukseen, mihin se on tarkoitettu, ellei turvallisuusluokan määrittäjä ole antanut muuhun suostumustaan. Sopimuksen 4 artiklan 1 kappale on sopusoinnussa lainkohdan kanssa.

Artiklan 2 kappaleen mukaan, mikäli sopimuspuoli tai sen 1 artiklassa tarkoitettuja asioita käsittelevä virasto tai oikeushenkilö tekee toisen sopimuspuolen alueella toimeenpantavan sopimuksen, johon liittyy turvallisuusluokiteltua tietoa, sopimuksen toimeenpanomaan sopimuspuoli vastaa tämän turvallisuusluokitellun tiedon hallinnoinnista omien normiensä ja vaatimustensa mukaisesti.

Artiklan 3 kappaleessa määritellään toimenpiteet, jotka sopimuspuolen on tehtävä ennen kuin se välittää toisilta sopimuspuolilta saamaansa turvallisuusluokiteltua tietoa lainkäyttövaltaansa kuuluville hankeosapuolille tai mahdollisille hankeosapuolille. Sopimuspuolen on a) varmistettava, että näillä hankeosapuolilla tai mahdollisilla hankeosapuolilla ja niiden organisaatioilla on valmiudet suojata turvallisuusluokiteltu tieto asianmukaisesti; b) tehtävä asianmukainen turvallisuus selvitys kyseisen hankeosapuolen organisaatioista sekä kaikista työntekijöistä, joiden tehtävät edellyttävät pääsyä turvallisuusluokiteltuun tietoon; c) varmistettava, että kaikille, joilla on pääsy turvallisuusluokiteltuun tietoon, tiedotetaan heidän velvollisuudestaan suojata turvallisuusluokiteltu tieto sovellettavan lainsäädännön mukaisesti; ja d) tehtävä määrääjain turvallisuustarkastuksia kyseisissä organisaatioissa, joista on tehty turvallisuus selvitys.

*5 artikla. Turvallisuusluokitukset.* Artiklassa määritellään, että turvallisuusluokiteltuun tietoon merkitään jokin seuraavista neljästä turvallisuusluokasta.

Korkein, ankarimpia tietoturvallisuustoimenpiteitä vaativa luokka on ”ERITTÄIN SALAINEN/YTTERST HEMLIG” (TOP SECRET). Suomessa luokkaan ”erittäin salainen” luetaan kuuluviksi tiedot, joiden luvaton ilmitulo voi aiheuttaa erittäin suurta vahinkoa maanpuolustukselle, turvallisuudelle, kansainvälisille suhteille tai muille yleisille eduille. Suomen kansainvälisiä suhteita suojaavat julkisuuslain 24 §:n 1 momentin 1

ja 2 kohta, maanpuolustusta momentin 10 kohta ja turvallisuutta momentin 5, 8 ja 9 kohdat. Muita määritelmässä tarkoitettuja yleisiä etuja voivat olla esimerkiksi valtionjohdon ja valtiovieraiden sekä tietojärjestelmien turvallisuusjärjestelyjen suojaaminen (24 § 1 mom. 7 kohta) sekä kansantalouden toimivuus (24 § 1 mom. 11 ja 12 kohta).

Toiseksi korkein turvallisuusluokka on ”SALAINEN/HEMLIG” (SECRET). Tähän kuuluvat Suomessa tiedot, joiden luvaton ilmitulo voi aiheuttaa merkittävää vahinkoa maanpuolustukselle, turvallisuudelle, kansainvälisille suhteille tai muille yleisille eduille.

Kolmanneksi korkein turvallisuusluokka on ”LUOTTAMUKSELLINEN / KONFIDENTIELL” (CONFIDENTIAL), jolla tarkoitetaan Suomessa tietoja, joiden luvaton ilmitulo voi aiheuttaa vahinkoa maanpuolustukselle, turvallisuudelle, kansainvälisille suhteille tai muille yleisille eduille.

Neljänteen turvallisuusluokkaan ”KÄYTTÖ RAJOITETTU/BEGRÄNSAD TILLGÅNG” (RESTRICTED) kuuluvat tiedot, joiden luvaton ilmitulo voi aiheuttaa haittaa yleisille eduille tai heikentää viranomaisen toimintaedellytyksiä.

Turvallisuusluokitusmerkintää koskevat erityissäännökset sisältyvät tietoturvallisuusasetuksen 11 §:ään, ja niiden vastaavuudesta kansainvälisen tietoturvallisuusveloitteen luokkien kanssa on säädetty asetuksen 12 §:ssä. Ruotsinkielisistä turvallisuusluokitusmerkinnöistä on erityissäännös asetuksen 11 §:n 4 momentissa.

Artiklan 2 kappaleen mukaan vastaanottava sopimuspuoli ei saa muuttaa vastaanottamansa turvallisuusluokitellun tiedon turvallisuusluokkaa ilman lähettävän sopimuspuolen kirjallista ennakkosuostumusta. Lähettävä sopimuspuoli ilmoittaa vastaanottavalle sopimuspuolelle vaihdetun tiedon turvallisuusluokan muutoksista.

Artiklan 3 kappaleen mukaan vastaanottava sopimuspuoli merkitsee saamaansa turvallisuusluokiteltuun tietoon oman vastaavan turvallisuusluokkansa. Käännöksiin ja kopioihin merkitään sama turvallisuusluokka kuin alkuperäiskappaleeseen.

Artiklan 4 kappaleen mukaan Ruotsista peräisin olevan tiedon, jossa on ainoastaan

merkintä HEMLIG, katsotaan kuuluvan turvallisuusluokkaan HEMLIG/SECRET. Luokitellun asiakirjan kopion merkitsemisestä on säädetty tietoturvallisuusasetuksen 17 § 2 momentissa.

*6 artikla. Toimivaltaiset turvallisuusviranomaiset ja turvallisuusyhteistyö.* Artiklan 1 kappaleessa määritellään, että toimivaltaiset turvallisuusviranomaiset valvovat sopimuksen täytäntöönpanoa. Artiklan 2 kappaleen mukaan sopimuspuolet ilmoittavat toisilleen nimeämänsä toimivaltaiset turvallisuusviranomaiset ja niiden muutokset.

Artiklan 3 kappaleessa todetaan, että toimivaltaiset turvallisuusviranomaiset toimittavat pyynnöstä toisilleen tietoja turvallisuusluokitellun tiedon suojaamista koskevista kansallisista laeistaan ja määräyksistään, normeistaan, menettelyistään ja käytännöistään, jotta voitaisiin saavuttaa ja ylläpitää toisiaan vastaavat turvallisuustasot. Tätä tarkoitusta varten toimivaltaiset turvallisuusviranomaiset voivat tehdä keskinäisiä vierailuja.

Artiklan 4 kappaleessa todetaan, että toimivaltaiset turvallisuusviranomaiset ilmoittavat toisilleen kulloinkin esiintyvistä turvallisuusriskeistä, jotka voivat vaarantaa välitetyn turvallisuusluokitellun tiedon.

Artiklan 5 ja 6 kappaleissa määritellään toimivaltaisten turvallisuusviranomaisten velvollisuus avustaa pyynnöstä toisiaan kansallisen lainsäädännön mukaisesti turvallisuuspalvelusten tekemisessä sekä ilmoittaa viipymättä toisilleen vastavuoroisesti tunnistettujen turvallisuuspalvelusten muutoksista.

Artiklan 7 kappaleen mukaan sopimuspuolten tiedustelu- tai turvallisuuspalvelut voivat kansallisen lainsäädännön mukaisesti vaihtaa suoraan keskenään operatiivisia tietoja tai tiedustelutietoja.

*7 artikla. Vierailut.* Artikla sisältää määräykset niistä menettelytavoista, joita noudatetaan järjestettäessä sopimuspuolten välillä vierailuja, joihin liittyy pääsy turvallisuusluokiteltuun tietoon tai alueille, joissa harjoitetaan turvallisuusluokiteltuun tietoon liittyvää toimintaa, tai säilytetään tai käsitellään turvallisuusluokiteltua tietoa. Artiklan 1 kappaleen mukaan vierailut edellyttävät isäntämaan toimivaltaisen turvallisuusviranomaisen antamaa kirjallista ennakkolupaa, mikäli niihin liittyy pääsy turvallisuusluokkaan

”CONFIDENTIAL”, tai sitä ylempään luokkaan kuuluvaan turvallisuusluokiteltuun tietoon tai alueille, joilla tällaista turvallisuusluokiteltua tietoa kehitetään, käsitellään tai säilytetään, tai saatetaan kehittää, käsitellä tai säilyttää.

Artiklan 2 kappaleen mukaan vierailun sallimisen edellytyksenä on, että vieraat lähettävän sopimuspuolen toimivaltainen viranomaisen on tehnyt vierailijoista turvallisuus selvityksen ja heillä on isäntävaltion kansallisten lakien ja määräysten mukainen lupa ottaa vastaan turvallisuusluokiteltua tietoa (esim. tiedonsaantitarve). Lisäksi vierailun sallimisen edellytyksenä on, että isäntäsopimuspuolen toimivaltainen viranomaisen on antanut vierailijoille luvan tarvittavaan yhteen tai useampaan vierailuun. Jälkimmäinen edellytys koskee vain niitä sopimuspuolia, joiden kansallinen järjestelmä edellyttää luvan antamista.

Vierailupyynnö (Request for Visit, RfV) esitetään 3 kappaleen mukaan isäntämaan toimivaltaiselle turvallisuusviranomaiselle vähintään 10 päivää ennen vierailua. Kiireellisissä tapauksissa toimivaltaiset turvallisuusviranomaiset voivat sopia lyhyemmästä ajasta. Tarkemmat määräykset tiedoista, jotka on sisällytettävä vierailupyynnöön, määritetään 4 kappaleessa, ja 5 kappaleessa todetaan, että vierailupyynnö toimitetaan noudattaen asianomaisten toimivaltaisten turvallisuusviranomaisten kesken sovittuja periaatteita.

Artiklan 6 kappaleen mukaan toistuvia vierailuja koskevat luvat ovat voimassa enintään 12 kuukautta. Artiklan 7 kappaleen mukaan isäntäsopimuspuoli voi tarvittaessa pyytää todistusta turvallisuuspalveluksesta. Muita vierailumenettelyjä voidaan 8 kappaleen mukaan soveltaa, jos asianomaisten sopimuspuolten toimivaltaiset turvallisuusviranomaiset sopivat siitä keskenään.

*8 artikla. Turvallisuusluokitellut sopimukset.* Artikla sisältää määräykset niitä tilanteita varten, joissa jokin sopimuspuoli tekee, taikka antaa luvan oman lainkäyttövaltansa piiriin kuuluvalla hankeosapuolelle tehdä, turvallisuusluokitellun sopimuksen toisen sopimuspuolen lainkäyttövallan piiriin kuuluvan hankeosapuolen kanssa.

Artiklan 1 kappaleen mukaan ennen turvallisuusluokitellun sopimuksen tekemistä toi-

sen sopimuspuolen maassa sopimuspuolen toimivaltainen turvallisuusviranomainen voi pyytää turvallisuusselvitystä, jonka toisen sopimuspuolen toimivaltainen turvallisuusviranomainen on tehnyt kyseisen hankeosapuolen organisaatiosta. Jollei turvallisuusselvitystä ole tehty, turvallisuusluokitellun sopimuksen tekävä sopimuspuoli voi pyytää hankeosapuolen edustamaa sopimuspuolta tekemään turvallisuusselvityksen kansallisten lakien ja määräysten mukaisesti. Artiklan 2 kappaleen mukaan kuitenkin silloin, kun kyse on avoimesta tarjouskilpailusta, jota ei ole suunnattu erityisesti mihinkään maahan tai yritykseen, vastaanottavan sopimuspuolen turvallisuusviranomainen voi toimittaa lähetettävän sopimuspuolen turvallisuusviranomaiselle asiaankuuluvat turvallisuustodistukset ilman tämän virallista pyyntöä. Määräyksen tarkoituksena on nopeuttaa suomalaisten tai vastavuoroisesti muiden pohjoismaisten yritysten pääsyä tarjouksen tekemiseen tarpeelliseen turvallisuusluokiteltuun tietoon, mikä puolestaan tehostaisi yritysten tarjousvalmistelua ja parantaisi niiden kilpailuasemaa.

Artiklan 3 kappaleen mukaan asianmukaiset turvallisuusmääräykset on kirjattava turvallisuusluokiteltuun sopimukseen ja sopimukseen on liitettävä asiakirjat, joissa määritetään kyseisessä sopimuksessa tarkoitetut turvallisuusluokitellut tiedot tai sen turvallisuusluokitellut osat tai osatekijät. Artiklan 4 kappaleessa määrätään turvallisuusluokitellun sopimuksen tekävän sopimuspuolen toimivaltaisen turvallisuusviranomaisen tehtäväksi varmistaa, että sopimuksen toimeenpannaan toimivaltaiselle turvallisuusviranomaiselle toimitetaan kopiot kaikista asianmukaisista sopimukseen liittyvistä turvallisuusasiakirjoista.

Turvallisuusluokiteltuja sopimuksia koskevat kansalliset säännökset sisältyvät kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 1 § 2 momenttiin (lain soveltaminen elinkeinonharjoittajaan), 2 §:n 2 kohtaan (erityissuojattava tietoaaineisto) sekä lain 3 lukuun, joka koskee tietoturvallisuustoimenpiteitä. Sopimuksen määräykset vastaavat tältä osin kansallista sääntelyä. Velvoitteen täyttämiseksi tarpeellisesta suomalaisen viranomaisen tietojenanto-oikeudesta säädetään kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 17 §:ssä.

*9 artikla. Turvallisuusluokitellun tiedon kääntäminen, kopiointi ja hävittäminen.*

Artikla sisältää määräykset siitä, miten eri turvallisuusluokkiin kuuluvia aineistoja saa kääntää, kopioida ja hävittää.

Artiklan 1 kappaleen mukaan kaikkiin turvallisuusluokitellun tiedon kopioihin ja käännöksiin tehdään asianmukainen turvallisuusluokitusmerkintä, ja ne suojataan kuten alkuperäinen turvallisuusluokiteltu tieto. Käännöksiä ja kopioita saadaan tehdä ainoastaan viralliseen tarkoitukseen tarvittava vähimmäismäärä. Artiklan 2 kappaleessa määrätään, että kaikkiin käännöksiin on tehtävä käännöskielineen merkintä siitä, että ne sisältävät turvallisuusluokiteltua tietoa. Vastaavat säännökset sisältyvät tietoturvallisuusasetuksen 17 §:ään.

Artiklan 3 kappaleessa edellytetään, että turvallisuusluokkaan TOP SECRET kuuluvaa tietoa ei saa kääntää eikä kopioida ilman aineiston lähettäneen sopimuspuolen siihen antamaa kirjallista lupaa. Artiklan 4 kappaleen mukaan luokkaan TOP SECRET kuuluvaa tietoa ei hävitetä ilman lähettävän sopimuspuolen kirjallista ennakkosuostumusta, vaan se palautetaan lähettävälle sopimuspuolelle sen jälkeen, kun sopimuspuolet eivät enää katso sitä tarvittavan. Määräyksen esimerkiksi tilanteissa, joissa aineisto tai sen osa on arkistolainsäädännön vuoksi säilytettävä. Turvallisuusluokkaan SECRET tai sitä alempaan turvallisuusluokkaan kuuluva tieto voidaan 5 kappaleen mukaan hävittää kansallisten lakien ja määräysten mukaisesti, kun vastaanottava sopimuspuoli ei enää katso sitä tarvittavan. Luokiteltujen asiakirjojen arkistoinnista säädetään arkistolaisissa (831/1994). Niiden hävittämistä koskevat säännökset sisältyvät tietoturvallisuusasetuksen 21 §:ään.

Artiklan 6 kappaleessa määrätään tilanteesta, jossa kriisitilanteen vuoksi on mahdollista suojata sopimuksen mukaisesti välitettyä turvallisuusluokiteltua tietoa. Näissä tapauksissa tieto hävitetään välittömästi ja vastaanottavan sopimuspuolen on ilmoitettava turvallisuusluokitellun tiedon hävittämisestä mahdollisimman pian lähettävän sopimuspuolen toimivaltaiselle turvallisuusviranomaiselle.

*10 artikla. Turvallisuusluokitellun tiedon välittäminen.* Artikla sisältää määräykset

menettelystä siirrettäessä turvallisuusluokiteltuja tietoja sopimuspuolten kesken. Artiklan 1 kappaleen mukaan tieto välitetään diplomaattiteitse tai kuriiritse, jolleivät asianomaiset toimivaltaiset turvallisuusviranomaiset muuta sovi. Artiklan 2 kappaleessa määrätään, että mikäli sopimuspuoli haluaa siirtää turvallisuusluokiteltua tietoa alueensa ulkopuolelle, siirrosta on sovittava ennakolta lähettävän sopimuspuolen kanssa. Määräys on sopusoinnussa turvallisuusluokitellun tiedon välittämistä koskevan tietoturvallisuusasetuksen 18 §:n kanssa.

*11 artikla. Tietoturvaloukkaus.* Artiklan 1 kappaleen mukaan todettaessa tietoturvaloukkaus, jonka johdosta sopimuksessa tarkoitettua turvallisuusluokiteltua tietoa katoaa tai ilmaistaan luvatta, sen maan toimivaltaisen turvallisuusviranomaisen, jossa loukkaus on tapahtunut, on ilmoitettava asiasta mahdollisimman pian asianomaisten sopimuspuolten toimivaltaisille turvallisuusviranomaisille. Toimivaltainen sopimuspuoli toteuttaa 2 kappaleen mukaan kansallisen lainsäädäntönsä mukaisesti kaikki asianmukaiset toimenpiteet rajoittaakseen tietoturvan loukkausten seurauksia sekä estääkseen loukkausten jatkumisen. Muut sopimuspuolet avustavat artiklan 3 kappaleen mukaan pyynnöstä tutkinnassa. Sopimuspuolille toimitetaan tieto tutkinnan tuloksista sekä loukkauksen johdosta toteutetuista toimenpiteistä. Lisäksi sopimuspuolille toimitetaan loppulausunto tietoturvaloukkauksen syistä, laajuudesta ja toimista, jotka on toteutettu tietoturvaloukkauksen uusimisen estämiseksi. Artiklan tarkoittamien velvoitteiden täytäntöön panemiseksi tarpeelliset säännökset sisältyvät kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 19 §:ään.

*12 artikla. Kustannukset.* Sopimuspuolet eivät korvaa toisilleen sopimuksesta mahdollisesti syntyneitä kustannuksia.

*13 artikla. Riitojen ratkaiseminen.* Kaikki sopimuksen tulkintaan tai soveltamiseen liittyvät sopimuspuolten väliset riidat ratkaistaan sopimuspuolten välisissä neuvotteluissa, eikä niitä saateta kansallisiin tai kansainvälisiin tuomioistuimiin tai kolmannen osapuolen ratkaistavaksi.

*14 artikla. Loppumääräykset.* Artiklassa on sopimuksen hyväksymistä, ratifiointia, voimaantuloa, muuttamista, ja irtisanomista

koskevat määräykset. Artiklan 1 kappaleen mukaan ratifioimis- tai hyväksymiskirjojen tallettaja on Norjan kuningaskunnan hallitus. Sopimus tulee artiklan 2 kappaleen mukaan voimaan kolmantenakymmenentenä päivänä siitä päivästä, jona viimeinen allekirjoittajahallitus on tallettanut ratifioimis- tai hyväksymiskirjansa. Artiklan 3 kappaleen mukaan sopimuspuoli voi kuitenkin voimaantuloon saakka ilmoittaa ratifioimis- tai hyväksymiskirjansa tallettaessaan tai myöhemmin, että se katsoo sopimuksen sitovan sitä sen suhteissa muuhun sopimuspuoleen, joka on tehnyt samanlaisen ilmoituksen. Nämä ilmoitukset tulevat voimaan kolmantenakymmenentenä päivänä siitä päivästä, jona ne on vastaanotettu. Määräyksen tarkoituksena on mahdollistaa sopimuksen soveltaminen väliaikaisesti sopimuspuolten näin halutessa ennen sen voimaantuloa niiden valtioiden välillä, jotka saavat kansallisen hyväksymismenettelynsä päätökseen nopeammin. Suomen on tarkoitus jättää sanotunlainen ilmoitus.

Artiklan 4 kappaleen mukaan sopimusta voidaan muuttaa kirjallisesti sopimuspuolten yhteisestä sopimuksesta. Artiklan 5 kappaleen mukaan hyväksytty muutos tulee voimaan kolmantenakymmenentenä päivänä siitä päivästä, jona viimeinen sopimuspuoli on ilmoittanut tallettajalle hyväksyneensä muutoksen. Artiklan 6 kappaleen mukaan sopimus on voimaantultuaan avoimna liittymistä varten kolmansille valtioille allekirjoittajahallitusten suostumuksella. Liittymisasiakirjat talletetaan Norjan kuningaskunnan hallituksen huostaan. Sopimukseen liittyvän valtion osalta sopimus tulee 7 kappaleen mukaan voimaan kolmantenakymmenentenä päivänä liittymisasiakirjojen tallettamispäivästä.

Sopimus on artiklan 8 kappaleen mukaan voimassa toistaiseksi. Sopimuspuoli voi milloin tahansa irtisanoa sopimuksen ilmoittamalla siitä kirjallisesti tallettajalle. Sopimuksen irtisanominen tulee voimaan irtisanoutuvan sopimuspuolen osalta kuuden kuukauden kuluttua irtisanomisilmoituksen tallettamisesta. Mikäli sopimus irtisanoetaan, sopimuksen määräysten mukaisesti välitetty turvallisuusluokiteltu tieto tai aineisto palautetaan artiklan 9 kappaleen mukaan mahdollisimman pian lähettävälle sopimuspuolelle. Sopimuksen irtisanomisesta huolimatta kaikki sopi-

muksen mukaisesti luovutettu palauttamaton turvallisuusluokiteltu tieto suojataan edelleen sopimuksen määräyksiä noudattaen. Artiklan 10 kappaleessa mainitaan ne sopimukset ja järjestelyt turvallisuusluokitellun tiedon suojaamiseksi, jotka sopimus korvaa tullessaan voimaan.

## 2 Lakiehdotuksen perustelut

Suomen perustuslain 95 §:ssä edellytetään, että kansainvälisen velvoitteen lainsäädännön alaan kuuluvat määräykset saatetaan valtion sisäisesti voimaan erityisellä voimaansaattamislailalla. Tällaiset määräykset tulee saattaa voimaan lailla myös silloin, kun velvoitteen johdosta ei ole tarpeen tarkistaa kansallisen lainsäädännön aineellista sisältöä. Koska Pohjoismaiden välinen tietoturvaluokitus sopimuksen velvoitteiden toteuttamiseksi ei aineellista lainsäädäntöä ole tarpeen muuttaa, esitys sisältää vain ehdotuksen blankettilaiksi.

1 §. Lakiehdotuksen 1 §:n säännöksellä saatettaisiin voimaan sopimuksen lainsäädännön alaan kuuluvat määräykset. Lainsäädännön alaan kuuluvia määräyksiä selostetaan jäljempänä eduskunnan suostumuksen tarpeellisuutta koskevassa jaksossa.

2 §. Lain voimaantulosta säädettäisiin tasavallan presidentin asetuksella. Lain on tarkoitus tulla voimaan samanaikaisesti kuin sopimus tulee Suomen osalta voimaan.

Pykälässä annettaisiin lisäksi tasavallan presidentille valtuus asetuksella säätää, että Suomi ilmoittaa ryhtyvänsä soveltamaan sopimusta jo ennen sen kansainvälistä voimaantuloa suhteissaan samanlaisen ilmoituksen tehneisiin sopimuspuoliin.

## 3 Voimaantulo

Suomen ja muiden Pohjoismaiden välisen sopimuksen 14 artiklan 1 kappaleen mukaan sopimuspuolet tallettavat hyväksymis- tai ratifioimiskirjansa Norjan kuningaskunnan hallituksen huostaan. Sopimus tulee voimaan kolmantenakymmenentenä päivänä siitä päivästä, jona viimeinen allekirjoittajahallitus on tallettanut ratifioimis- tai hyväksymiskirjansa.

Sopimuksen 14 artiklan 3 kappaleen mukaan sopimuspuoli voi myös ilmoittaa, että

se katsoo sopimuksen sitovan itseään suhteissa muihin sopimuspuoliin, jotka ovat tehneet vastaavanlaisen ilmoituksen. Ilmoitukset tulevat voimaan kolmantenakymmenentenä päivänä siitä päivästä, jona ne on vastaanotettu. Tarkoituksena on, että Suomi antaisi tällaisen ilmoituksen, joka mahdollistaisi sopimuksen määräysten soveltamisen väliaikaisesti ennen sen voimaantuloa suhteessa vastaavanlaisen ilmoituksen tehneisiin sopimuspuoliin nähden. Tällaisia olisivat alustavan tiedon mukaan ainakin Ruotsi ja Norja.

Sopimuksen voimaansaattamislaki on tarkoitettu tulemaan voimaan tasavallan presidentin asetuksella säädettävänä ajankohtana samaan aikaan, kuin sopimus tulee Suomen osalta voimaan.

Yleinen turvallisuus sopimus korvaa voimaan tullessaan pohjoismaisen turvallisuusmateriaalialan yhteistyösopimuksen puitteissa laaditun turvallisuussuojaa koskevan yhteisymmärryksen Tanskan, Suomen, Norjan ja Ruotsin välillä.

Voimaansaattamislain 2 §:ssä annettaisiin tasavallan presidentille valtuus asetuksella säätää, että Suomi ilmoittaa ryhtyvänsä soveltamaan sopimusta jo ennen sen kansainvälistä voimaantuloa suhteissaan samanlaisen ilmoituksen tehneisiin sopimuspuoliin.

## 4 Eduskunnan suostumuksen tarpeellisuus ja käsittelyjärjestys

### 4.1 Eduskunnan suostumuksen tarpeellisuus

Perustuslain 94 §:n 1 momentin mukaan eduskunta hyväksyy sellaiset valtiosopimukset ja muut kansainväliset velvoitteet, jotka sisältävät lainsäädännön alaan kuuluvia määräyksiä. Perustuslakivaliokunnan tulkintakäytännön mukaan määräys on luettava lainsäädännön alaan kuuluvaksi, jos se koskee jonkin perustuslaissa turvatun perusoikeuden käyttämistä tai rajoittamista, jos määräys muutoin koskee yksilön oikeuksien ja velvollisuuksien perusteita, jos määräyksen tarkoituksesta asiasta on perustuslain mukaan säädettävä lailla, tai jos määräyksessä tarkoitusta asiasta on jo voimassa lain säännöksiä, taikka siitä on Suomessa vallitsevan käsityksen mukaan säädettävä lailla. Perustuslakiva-



liokunnan mukaan kansainvälisen velvoitteen määräys kuuluu näiden perusteiden mukaan lainsäädännön alaan siitä riippumatta, onko määräys ristiriidassa vai sopusoinnussa Suomessa lailla annetun säännöksen kanssa (kts. esimerkiksi PeVL 11/2000 vp ja PeVL 12/2000 vp).

Edellä mainituilla perusteilla esitykseen sisältyvässä sopimuksessa on lukuisia eduskunnan hyväksymistä edellyttäviä määräyksiä. Sopimuksen 1 artiklassa määrätään sopimuksen tarkoituksesta ja soveltamisalasta. Sopimuksen 2 artiklassa määritellään, mitä tarkoitetaan turvallisuusluokitellulla tiedolla, lähettävällä sopimuspuolella, vastaanottavalla sopimuspuolella, turvallisuusluokitellulla sopimuksella, toimivaltaisella turvallisuusviranomaisella, hankeosapuolella, tietoturvaloukkauksella, turvallisuusselvityksellä, tiedonsaantitarpeella ja kolmannella osapuolella. Koska nämä sopimusmääräykset vaikuttavat joko suoraan tai välillisesti sopimuksen lainsäädännön alaan kuuluvien aineellisten määräysten tulkintaan ja soveltamiseen, ne edellyttävät eduskunnan hyväksymistä (PeVL 6/2001 vp).

Sopimuksen 3 artiklan 1 kappaleessa edellytetään, että sopimuspuolet toteuttavat kansallisen lainsäädäntönsä mukaisesti asianmukaiset toimet turvallisuusluokitellun tiedon suojaamiseksi ja sitoutuvat siten suojaamaan tietoa samantasoisesti, kuin omaa vastaavaan turvallisuusluokkaan kuuluvaa tietoaan. Tämä edellyttää vastaanotetun turvallisuusluokitellun tiedon merkitsemistä asianmukaisesti. Laissa kansainvälisistä tietoturvaluusvelvoitteista säädetään viranomaisten toimenpiteistä kansainvälisten tietoturvaluusvelvoitteiden toteuttamiseksi. Lain 8 §:ssä veloitetaan viranomaista merkitsemään turvallisuusluokka erityissuojattavaan tietoaan. Määräys kuuluu lainsäädännön alaan.

Turvallisuusluokiteltua tietoa koskeva ilmaisu- ja käyttörajoitus on ilmaistu sopimuksen 4 artiklassa. Artiklassa määrätään velvollisuudesta suojata sopimuksen soveltamisalan piiriin kuuluva turvallisuusluokiteltu tieto kansallisin toimenpitein, jotka rajoittavat turvallisuusluokitellun tiedon välittämistä, käyttämistä ja pääsyä siihen. Vastaanottava sopimuspuoli ei saa luovuttaa turvallisuusluokiteltua tietoa, ellei asiasta ole sovittu kirjallisesti lähettävän sopimuspuolen kanssa.

Suomessa viranomaisten asiakirjojen julkisuus on pääsääntö. Jokaisella on perustuslain 12 §:n 2 momentin mukaan oikeus saada tieto viranomaisen julkisesta asiakirjasta. Tätä oikeutta voidaan rajoittaa välttämättömistä syistä vain lailla. Yleisesti sovellettavat säännökset salassapito- ja luokitusmerkinnästä on säädetty julkisuuslain 25 §:ssä. Pykälän mukaan salassa pidettävään viranomaisen asiakirjaan on tehtävä merkintä asiakirjan salassapitamisesta, kun tällainen asiakirja annetaan asianosaiselle, ja kun asiakirja on pidettävä salassa toisen tai yleisen edun vuoksi. Muihin salaisiin asiakirjoihin tehtävä merkintä on harkinnanvarainen.

Julkisuuslain säännöksistä poiketen kansainvälisistä tietoturvaluusvelvoitteista annetun lain 6 §:n 1 momentissa, sen 1 päivänä marraskuuta 2010 voimaantulleessa muodossa (885/2010) erityissuojattava tietoaaineisto on pidettävä salassa, jollei kansainvälisestä tietoturvaluusvelvoitteesta muuta johdu. Hallituksen esityksessä muutosta perusteltiin Suomen käymissä sopimusneuvotteluissa syntyneillä tilanteilla, joissa toinen sopimuspuoli ei takaa sopimuksen perusteella ehdotonta salassapitoa, vaan joissa asia jää kansalliseen lainsäädäntöön perustuvan tapauskohtaisen vahinkoedellytysharkinnan varaan. Tarkoituksenmukaista ei ole, että Suomi noudattaa laajempaa salassapitovelvollisuutta, kuin toiset sopimuspuolet. Tästä syystä ehdotettiin, että pykälän 1 momenttiin otetaan lauseke, jonka mukaan salassapitovelvollisuus olisi riippuvainen kunkin sopimuksen tai muun kansainvälisen velvoitteen sisällöstä. Muutoksella varauduttaisiin tulevien kansainvälisten sopimusten, kuten nyt käsillä olevan Pohjoismaiden välillä tehdyn sopimuksen, käsittelyyn. Sopimusmääräys on siten sopusoinnussa voimassa olevan 6 §:n 1 momentin säännösten kanssa.

Samaisen lain 8 §:ssä on säännökset turvallisuusluokan merkitsemisestä erityissuojattavaan tietoaan. Sen mukaisesti erityissuojattavaan tietoaan on julkisuuslain säännöksistä riippumatta tehtävä kansainvälisessä tietoturvaluusvelvoitteesta määritelty merkintä sen osoittamiseksi, millaisia tietoturvaluusvaatimuksia käsittelyssä on noudatettava. Sopimusmääräykset asettavat näin ollen Suomen julkisuuslakia tiukemmat vaatimukset turvallisuusluokitellun tiedon mer-

kitsemiselle. Määräykset edellyttävät eduskunnan hyväksymistä. Edelleen 4 artiklan 3 kappaleen b kohdassa määrätään sopimuspuolten velvollisuudesta teettää asianmukainen turvallisuus selvitys henkilöistä, joilla on pääsy sopimuksessa tarkoitettuun turvallisuusluokiteltuun tietoon. Turvallisuus selvitysten laadinnassa on otettava huomioon perustuslain 10 §:n 1 momentissa säädetty yksityiselämän suoja ja velvollisuus säätää henkilötietojen suojasta lailla. Suomessa turvallisuus selvityksen kohteena olevista henkilöistä sekä selvityksessä sovellettavasta menettelystä on säädetty turvallisuus selvityksistä annetussa laissa.

Sopimuksen 7 artiklassa on määräykset toisen sopimuspuolen luonnollisten henkilöiden vierailuista isäntäsopimuspuolen tiloihin, joissa käsitellään turvallisuusluokiteltua tietoa. Sopimuspuolen edustajien vierailuiden tarkoituksena on varmistaa sopimuksen toteuttaminen turvallisuusluokiteltujen tietojen asianmukaiseksi suojaamiseksi. Tähän vierailuoikeuteen ei sisälly sellaista julkista vallan käyttöä ja tarkastusoikeutta, joka olisi ristiriidassa perustuslain kanssa (PeVL 179/1997). Sopimus määräys luo välillisesti myös yksityisille tilausten saajille velvollisuuden sallia vierailut omiin toimitiloihinsa. Kansainvälisistä tietoturvaluusvelvoitteista annetun lain 18 §:ssä on vastaatvat säännökset vierailuja koskevan sopimus määräyksen täytäntöönpanoon liittyvistä seikoista.

Sopimuksen 8 artiklassa on määräykset turvallisuusluokitelluista sopimuksista ja niihin tarvittavista turvallisuus selvityksistä. Yhteisöturvallisuus selvitystä koskevat säännökset sisältyvät kansainvälisistä tietoturvaluusvelvoitteista annetun lain 12 ja 13 §:ään, joten määräyksen on katsottava kuuluvan lainsäädännön alaan.

Sopimuksen 9 artiklassa on määräykset turvallisuusluokitellun tiedon kääntämisestä, kopioinnista ja hävittämisestä. Turvallisuusluokitellun tiedon arkistoinnista säädetään arkistolaisissa. Sen sijaan aineiston kopioimista koskevat säännökset sisältyvät tietoturvaluusasetuksen 17 §:ään ja hävittämistä koskevat säännökset asetuksen 21 §:ään, joten niiltä osin määräykset eivät edellytä eduskunnan suostumusta. Sopimuksen 11 artiklassa edellytetään, että sopimuspuoli ilmoit-

taa viipymättä asianomaisille sopimuspuolille, jos tietoturvaluokituksen todetaan tapahtuneen. Sopimuspuolten on tutkittava turvallisuusluokitellun tiedon suojaamista koskevien säännösten rikkominen, sekä ryhdyttävä mahdollisuuksien mukaan toimenpiteisiin tietoturvaluokituksen seurausten rajoittamiseksi ja loukkauksen jatkumisen estämiseksi, sekä annettava toisilleen tarvittaessa tutkintaa apua. Kansainvälisistä tietoturvaluusvelvoitteista annetun lain 19 §:ssä säädetään kansallisen turvallisuusviranomaiselle kuuluvista velvoitteista sopimus määräyksissä tarkoitetuissa tilanteissa.

## 4.2 Käsittelyjärjestys

Käsittelyjärjestyksen kannalta merkityksellisiä sopimus määräyksiä sisältyy sopimuksen 4 artiklaan, joka asettaa rajoituksia turvallisuusluokitellun tiedon tai materiaalin julkisuudelle. Sopimus määräykset ovat merkityksellisiä perustuslain 12 §:n 2 momentin suojaaman, julkisuusperiaatteelle rakentuvan tiedonsaantioikeuden kannalta. Tätä tiedonsaantioikeutta saa rajoittaa vain lailla ja vain välttämättömistä syistä. Tällaisena välttämättömänä syynä voidaan pitää sen turvaamista, että Suomi ja suomalaiset yritykset voivat osallistua sellaisiin kansainvälisiin sekä Pohjoismaiden välisiin toimintoihin ja hankkeisiin, joiden toteuttaminen edellyttää arkaluonteisten salassa pidettävien tietojen vaihtoa. Salassapitoa koskeva erityissäännös on otettu kansainvälisistä tietoturvaluusvelvoitteista annetun lain 6 §:ään.

Pohjoismaiden välillä turvallisuusluokittelun tiedon vastavuoroisesta suojaamisesta ja vaihtamisesta tehtyyn sopimukseen ei voida katsoa sisältyvän sellaisia määräyksiä, jotka koskisivat perustuslakia sen 94 §:n 2 momentissa ja 95 §:n 2 momentissa tarkoitettulla tavalla. Hallituksen näkemyksen mukaan sopimus voitaisiin näin ollen hyväksyä äänten enemmistöllä ja ehdotus sen lainsäädännön alaan kuuluvien sopimus määräysten voimaansaattamiseksi tavallisen lain säätämiskäytännössä.

Edellä olevan perusteella ja perustuslain 94 §:n mukaisesti esitetään,

*että Eduskunta hyväksyisi Osllossa 7 päivänä toukokuuta 2010 Tanskan, Suomen, Islannin, Norjan ja Ruotsin välillä turvallisuusluokitellun tiedon vastavuoroisesta suojaamisesta ja vaihtamisesta tehdyn yleisen turvallisuussopimuksen.*

Koska sopimus sisältää määräyksiä, jotka kuuluvat lainsäädännön alaan, annetaan samalla Eduskunnan hyväksyttäväksi seuraava lakiehdotus:

## Laki

### Tanskan, Suomen, Islannin, Norjan ja Ruotsin välillä tehdyn yleisen turvallisuussopimuksen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta

Eduskunnan päätöksen mukaisesti säädetään:

#### 1 §

Turvallisuusluokitellun tiedon vastavuoroisesta suojaamisesta ja vaihtamisesta Tanskan, Suomen, Islannin, Norjan ja Ruotsin välillä Osllossa 7 päivänä toukokuuta 2010 tehdyn yleisen turvallisuussopimuksen lainsäädännön alaan kuuluvat määräykset ovat lakina voimassa sellaisina kuin Suomi on niihin sitoutunut.

#### 2 §

Tämän lain voimaantulosta säädetään tasavallan presidentin asetuksella. Tasavallan presidentin asetuksella voidaan säätää, että tätä lakia sovelletaan ennen sopimuksen voimaantuloa suhteissa niihin sopimuspuoliin, jotka ovat ilmoittaneet tai ilmoittavat soveltavansa sopimusta ennen sen voimaantuloa suhteissa niihin sopimuspuoliin, jotka ovat tehneet samanlaisen ilmoituksen.

---

Helsingissä 5 päivänä marraskuuta 2010

**Tasavallan Presidentti**

**TARJA HALONEN**

Ulkoasiainministeri *Alexander Stubb*

*Sopimusteksti*

**YLEINEN  
TURVALLISUUSSOPIMUS**

**TANSKAN,  
SUOMEN,  
ISLANNIN,  
NORJAN  
JA  
RUOTSIN**

**VÄLILLÄ**

**TURVALLISUUSLUOKITELLUN  
TIEDON VASTAVUOROISESTA  
SUOJAAMISESTA JA  
VAIHTAMISESTA**

Tanskan kuningaskunnan hallitus, Suomen tasavallan hallitus, Islannin hallitus, Norjan kuningaskunnan hallitus ja Ruotsin kuningaskunnan hallitus ja, jäljempänä ”sopimuspuolet”, jotka haluavat turvata sellaisen turvallisuusluokitellun tiedon, jota sopimuspuolet vaihtavat suoraan keskenään, tai jota vaihdetaan sopimuspuolten lainkäyttövaltaan kuuluvien muiden valtion viranomaisten, tai turvallisuusluokiteltua tietoa käsittelevien julkis- tai yksityisoikeudellisten oikeushenkilöiden kautta, ovat sopineet seuraavasta:

**1 artikla**

*Tarkoitus ja soveltamisala*

(1) Tämän sopimuksen tarkoituksena on suojata turvallisuusluokiteltua tietoa, jota kaksi tai useampia sopimuspuolia vaihtaa keskenään tai jota sopimuspuolten lainkäyttövaltaan kuuluvat hankeosapuolet vaihtavat keskenään ulko-, puolustus-, turvallisuus- tai poliisiasioissa tai tiede-, elinkeino- ja teknologiayhteistyössä, tai jota tuotetaan tai syntyy vaihdettavan tiedon perusteella.

(2) Sopimuspuoli ei voi vedota tähän sopimukseen saadakseen turvallisuusluokiteltua tietoa, jota muut sopimuspuolet ovat saaneet kolmannelta osapuolelta.

**GENERAL SECURITY  
AGREEMENT ON THE MUTUAL  
PROTECTION AND EXCHANGE  
OF CLASSIFIED INFORMATION**

**BETWEEN**

**DENMARK,  
FINLAND,  
ICELAND,  
NORWAY  
AND  
SWEDEN**

The Government of the Kingdom of Denmark, the Government of the Republic of Finland, the Government of Iceland, the Government of the Kingdom of Norway and the Government of the Kingdom of Sweden, hereafter called the Parties, in order to safeguard any Classified Information exchanged directly or through other State bodies or public or private legal entities that deal with Classified Information under the jurisdiction of the Parties, have agreed upon the following:

**Article 1**

*Purpose and scope of application*

(1) The purpose of this Agreement is to protect Classified Information exchanged between two or more of the Parties, or between Contractors under the jurisdiction of the Parties, in the areas of foreign affairs, defence, security, police or scientific, industrial and technological cooperation, or produced on the basis of, or arising from, exchanged information.

(2) This Agreement may not be invoked by a Party in order to obtain Classified Information that other Parties have received from a Third Party.

## 2 artikla

*Määritelmät*

(1) Tässä sopimuksessa tarkoitetaan *turvallisuusluokitellulla tiedolla* missä tahansa muodossa olevaa tietoa, joka on suojattava katoamiselta, luvattomalta ilmaisemiselta tai muulta vaarantumiselta ja joka on merkitty turvallisuusluokitelluksi; *lähettävällä sopimuspuolella* sopimuspuolta tai sen lainkäyttövaltaan kuuluvaa muuta valtion viranomaista tai julkis- tai yksityisoikeudellista oikeushenkilöä, joka välittää turvallisuusluokiteltua tietoa; *vastaanottavalla sopimuspuolella* sopimuspuolta tai muuta sen lainkäyttövaltaan kuuluvaa valtion viranomaista tai julkis- tai yksityisoikeudellista oikeushenkilöä, jolle lähettyvä sopimuspuoli välittää turvallisuusluokiteltua tietoa; *turvallisuusluokitellulla sopimuksella* sopimusta, johon sisältyy tai liittyy turvallisuusluokiteltua tietoa; *toimivaltaisella turvallisuusviranomaisella* turvallisuusasioista vastaavaa hallituksen viranomaista; *hankeosapuolella* luonnollista henkilöä tai oikeushenkilöä, joka on oikeustoimikelpoinen tekemään sopimuksia; *tietoturvaloukkauksella* kansallisten turvallisuusmääräysten vastaista tekoa tai laiminlyöntiä, jonka johdosta turvallisuusluokiteltu tieto saattaa vaarantua tai olla vaarassa paljastua; *turvallisuusselvityksellä* tutkintamenettelyyn perustuvaa myönteistä arviota siitä, että luonnolliselle henkilölle tai oikeushenkilölle voidaan sallia pääsy tiettyyn turvallisuusluokkaan kuuluvaan turvallisuusluokiteltuun tietoon, sekä antaa oikeus käsitellä sitä asianomaisten kansallisten turvallisuusmääräysten mukaisesti; *tiedonsaantitarpeella* periaatetta, jonka mukaan luonnollisille henkilöille voidaan sallia pääsy turvallisuusluokiteltuun tietoon ainoastaan heidän virkavelvollisuuksiensa tai tehtäviensä yhteydessä; *kolmannella osapuolella* toimielintä, kansainvälistä tai kansallista järjestöä, oikeushenkilöä tai valtiota, joka ei ole tämän sopimuksen sopimuspuoli.

## Article 2

*Definitions*

(1) For the purpose of this Agreement: *Classified Information* means information, regardless of its form, that under the laws of either Party requires protection against loss, unauthorised disclosure or other compromise and has been so designated; *Originating Party* means the Party, as well as any other State bodies or public or private legal entities under its jurisdiction, releasing Classified Information; *Receiving Party* means the Party, as well as any other State bodies or public or private legal entities under its jurisdiction, to which Classified Information is released by the Originating Party; *Classified Contract* means a contract which contains or involves Classified Information; *Competent Security Authority* means any Government authority responsible for security issues; *Contractor* means an individual or a legal entity possessing the legal capability to undertake contracts; *Breach of Security* means an act or an omission contrary to national security regulations the result of which may endanger or compromise Classified Information; *Security Clearance* means a positive determination following an investigative procedure to ascertain the eligibility of a person or entity to have access to and to handle Classified Information on a certain level in accordance with the relevant national security regulations; *"Need to Know"* means a principle by which access to Classified Information may only be granted to individuals in connection with their official duties or tasks; *Third Party* means any institution, international or national organisation, legal entity or State that is not a Party to this Agreement.

Tämän sopimuksen sopimuspuolta pidetään ”kolmantena osapuolena” yhteistyössä, johon kyseinen sopimuspuoli ei osallistu.

A Party to this Agreement is considered as a “Third Party” regarding co-operation activities in which the Party does not participate.

## 3 artikla

## Article 3

*Turvallisuusluokitellun tiedon suojaaminen**Protection of Classified Information*

(1) Sopimuspuolet toteuttavat kansallisen lainsäädäntönsä mukaisesti asianmukaiset toimet suojatakseen tässä sopimuksessa tarkoitettua turvallisuusluokitellun tiedon. Sopimuspuolet antavat kaikelle tässä sopimuksessa tarkoitettulle turvallisuusluokitellulle tiedolle samantasoinen suojan, kuin omalle vastaavaan 5 artiklan mukaiseen turvallisuusluokkaan kuuluvalla tiedolle.

(1) The Parties shall take appropriate measures, in accordance with their national legislation, to protect Classified Information under this Agreement. The Parties shall afford to all Classified Information under this Agreement the same degree of security protection as is provided to their own Classified Information of equivalent level of classification, as defined in Article 5.

(2) Pääsy turvallisuusluokkaan CONFIDENTIAL tai sitä ylempään luokkaan kuuluvaan turvallisuusluokiteltuun tietoon, sekä paikkoihin ja tiloihin, joissa säilytetään turvallisuusluokiteltua tietoa tai harjoitetaan turvallisuusluokiteltuun tietoon liittyvää toimintaa, sallitaan ainoastaan henkilöille, joista on tehty turvallisuusselvitys ja joilla on tiedon-saantitarve.

(2) Access to Classified Information on the level CONFIDENTIAL or above, and to locations and facilities where Classified Information is stored or activities involving Classified Information are performed, shall be limited to those who have been granted a Security Clearance and who have a Need to Know.

(3) Tämän sopimuksen perusteella sopimuspuolet tunnustavat vastavuoroisesti toistensa tekemät turvallisuusselvitykset.

(3) Within the framework of this Agreement the Parties shall mutually recognise each others' Security Clearances.

(4) Sopimuspuolet valvovat turvallisuuslainsäädännön, -määräysten ja käytäntöjen noudattamista lainkäyttövaltaansa kuuluvissa virastoissa, toimistoissa ja tiloissa, joissa säilytetään, kehitetään, tuotetaan ja/tai käytetään toisten sopimuspuolten turvallisuusluokiteltua tietoa.

(4) Each Party shall supervise the observance of security laws, regulations and practices at agencies, offices and facilities within their jurisdiction that possess, develop, produce and/or use Classified Information of other Parties.

## 4 artikla

## Article 4

*Turvallisuusluokitellun tiedon ilmaiseminen ja käyttö**Disclosure and use of Classified Information*

(1) Sopimuspuolet noudattavat luovuttajan suostumuksen periaatetta perustuslakiensa sekä muiden kansallisten lakiensa ja määräystensä mukaisesti eivätkä ilmaise tässä sopimuksessa tarkoitettua turvallisuusluokiteltua tietoa kolmansille osapuolille tai muiden maiden kansalaisille sopimatta asiasta ensin kirjallisesti lähettävän sopimuspuolen kanssa. Sopimuspuolen toisille sopimuspuolille välittämää turvallisuusluokiteltua tietoa saa käyttää ainoastaan sille määrättyyn tarkoitukseen.

(1) The Parties shall respect the principle of originator consent in accordance with their constitutional requirements, national laws and regulations, and not disclose Classified Information under this Agreement to Third Parties or nationals of other countries without prior written consultation with the Originating Party. Classified Information released by one Party to other Parties shall be used for the specified purpose only.

(2) Jos sopimuspuoli ja/tai sen 1 artiklassa tarkoitettuja asioita käsittelevä virasto tai oikeushenkilö tekee toisen sopimuspuolen alueella toimeen pantavan sopimuksen, johon liittyy turvallisuusluokiteltua tietoa, sopimuksen toimeenpanomaan sopimuspuoli vastaa tämän turvallisuusluokitellun tiedon hallinnoinnista omien normiensa ja vaatimustensa mukaisesti.

(3) Ennen kuin vastaanottava sopimuspuoli välittää toisilta sopimuspuolilta saamaansa turvallisuusluokiteltua tietoa lainkäyttövaltaansa kuuluville hankeosapuolille tai mahdollisille hankeosapuolille, se

a. varmistaa, että näillä hankeosapuolilla tai mahdollisilla hankeosapuolilla ja niiden organisaatioilla on valmiudet suojata turvallisuusluokiteltu tieto asianmukaisesti;

b. tekee asianmukaisen turvallisuusselvityksen kyseisen hankeosapuolen organisaatioista, sekä kaikista sen työntekijöistä, joiden tehtävät edellyttävät pääsyä turvallisuusluokiteltuun tietoon;

c. varmistaa, että kaikille, joilla on pääsy turvallisuusluokiteltuun tietoon, tiedotetaan heidän velvollisuudestaan suojata turvallisuusluokiteltu tieto sovellettavan lainsäädännön mukaisesti; ja

d. tekee määräjain turvallisuustarkastuksia kyseisissä organisaatioissa, joista on tehty turvallisuusselvitys.

#### 5 artikla

##### *Turvallisuusluokitukset*

(1) Turvallisuusluokiteltuun tietoon merkitään jokin seuraavista turvallisuusluokista:

(2) In the event that a Party and/or its agencies or entities concerned with subjects set out in Article 1 award a contract for performance within the territory of one of the other Parties and such contract involves Classified Information, the Party of the country in which the performance under the contract is to take place shall assume responsibility for administering such Classified Information in accordance with its own standards and requirements.

(3) The Receiving Party, prior to the release of any Classified Information received from other Parties to Contractors or prospective Contractors under its jurisdiction, shall:

a. ensure that such Contractors or prospective Contractors and their facilities have the capability to protect the Classified Information adequately;

b. grant an appropriate Security Clearance to the relevant Contractor's facilities and to all its personnel whose duties require access to the Classified Information;

c. ensure that all persons having access to the Classified Information are informed of their responsibilities to protect the Classified Information in accordance with the applicable laws;

d. carry out periodic security inspections of relevant security cleared facilities.

#### Article 5

##### *Security classifications*

(1) Classified Information shall be marked with one of the following security classification levels:



Englanniksi	“TOP SECRET”	“SECRET”	“CONFIDENTIAL”	“RESTRICTED”
<b>TANSKA</b>	YDERST HEMMELIGT	HEMMELIGT	FORTROLIGT	TIL TJENESTEBRUG
<b>SUOMI</b>	ERITTÄIN SALAINEN / YTTERST HEMLIG	SALAINEN/ HEMLIG	LUOTTA- MUKSELLINEN/ KONFIDENTIELL	KÄYTTÖ RAJOITETTU/ BEGRÄNSAD TILLGÅNG
<b>ISLANTI</b>	ALGJORT LEYNDARMAL	LEYNDARMAL	TRUNADARMAL	TAKMARKADUR ADGANGUR
<b>NORJA</b>	STRENGT HEMMELIG	HEMMELIG	KONFIDENSIELT	BEGRENSET
<b>RUOTSI</b> PUOLUSTUS- VIRANOMAISET	HEMLIG/ TOP SECRET	HEMLIG/ SECRET	HEMLIG/ CONFIDENTIAL	HEMLIG/ RESTRICTED
MUUT VIRANOMAISET	HEMLIG AV SYNNERLIG BETYDELSE FÖR RIKETS SÄKERHET	HEMLIG	-	-

(2) Vastaanottava sopimuspuoli ja/tai sen virastot tai oikeushenkilöt eivät saa muuttaa vastaanottamansa turvallisuusluokitellun tiedon turvallisuusluokkaa ilman lähettävän sopimuspuolen kirjallista ennakkosuostumusta. Lähettävä sopimuspuoli ilmoittaa vastaanotavalle sopimuspuolelle vaihdetun tiedon turvallisuusluokituksen muutoksista.

(3) Vastaanottava sopimuspuoli merkitsee saamaansa turvallisuusluokiteltuun tietoon oman vastaavan turvallisuusluokkansa. Käännöksiin ja kopioihin merkitään sama turvallisuusluokka kuin alkuperäiskappaleeseen.

(4) Ruotsista peräisin olevan tiedon, jossa on ainoastaan merkintä HEMLIG, katsotaan kuuluvan turvallisuusluokkaan HEMLIG/SECRET.

(2) The Receiving Party and/or its agencies or entities shall not change the security classification level of received Classified Information without the prior written consent of the Originating Party. The Originating Party shall inform the Receiving Party of any changes in the security classification of the exchanged information.

(3) The Receiving Party shall mark the received Classified Information with its own equivalent security classification level. Translations and reproductions shall be marked with the same security classification level as the original.

(4) Information from Sweden bearing the sole marking “HEMLIG” shall be regarded as HEMLIG/SECRET.

## 6 artikla

*Toimivaltaiset turvallisuusviranomaiset ja turvallisuusyhteistyö*

(1) Toimivaltaiset turvallisuusviranomaiset valvovat tämän sopimuksen täytäntöönpanoa.

(2) Sopimuspuolet ilmoittavat toisilleen nimeämänsä toimivaltaiset turvallisuusviranomaiset ja niiden muutokset.

(3) Toisiaan vastaavien turvallisuustasojen saavuttamiseksi ja ylläpitämiseksi toimivaltaiset turvallisuusviranomaiset toimittavat pyynnöstä toisilleen tietoja turvallisuusluokitellun tiedon suojaamista koskevista kansallisista laeistaan ja määräyksistään, normeistaan, menettelyistään ja käytännöistään. Tätä tarkoitusta varten toimivaltaiset turvallisuusviranomaiset voivat tehdä keskinäisiä vierailuja.

(4) Toimivaltaiset turvallisuusviranomaiset ilmoittavat toisilleen kulloinkin esiintyvistä turvallisuusriskeistä, jotka voivat vaarantaa välitetyn turvallisuusluokitellun tiedon.

(5) Toimivaltaiset turvallisuusviranomaiset avustavat pyynnöstä toisiaan kansallisen lainsäädännön mukaisesti turvallisuus selvitysten tekemisessä.

(6) Toimivaltaiset turvallisuusviranomaiset ilmoittavat viipymättä toisilleen vastavuoroisesti tunnustettujen turvallisuus selvitysten muutoksista.

(7) Sopimuspuolten tiedustelu- ja/tai turvallisuuspalvelut voivat kansallisen lainsäädännön mukaisesti vaihtaa suoraan keskenään operatiivisia tietoja ja/tai tiedustelutietoja.

## 7 artikla

*Vierailut*

(1) Vierailut edellyttävät isäntä sopimuspuolen toimivaltaisen turvallisuusviranomaisen antamaa kirjallista ennakkolupaa, jos niihin liittyy pääsy turvallisuusluokkaan CONFIDENTIAL, tai sitä ylempään luokkaan kuuluvaan turvallisuusluokiteltuun tietoon tai alueille, joilla tällaista turvallisuusluokiteltua tietoa kehitetään, käsitellään tai säilytetään tai saatetaan kehittää, käsitellä tai säilyttää.

## Article 6

*Competent Security Authorities and Security Cooperation*

(1) The Competent Security Authorities shall supervise the implementation of this Agreement.

(2) The Parties shall notify each other of the designation of their Competent Security Authorities and any changes thereto.

(3) In order to achieve and maintain comparable standards of security, the Competent Security Authorities shall, on request, provide each other with information about their national laws and regulations, standards, procedures and practices for the protection of Classified Information. To this aim the Competent Security Authorities may visit each other.

(4) The Competent Security Authorities shall inform each other of any relevant security risks that may endanger released Classified Information.

(5) On request, the Competent Security Authorities shall, in accordance with national legislation, assist each other in carrying out Security Clearance procedures.

(6) The Competent Security Authorities shall promptly inform each other about any changes in mutually recognized Security Clearances.

(7) The intelligence and security services of the Parties may, in accordance with national legislation, exchange operative and/or intelligence information directly with each other.

## Article 7

*Visits*

(1) Visits entailing access to Classified Information classified as CONFIDENTIAL or above, or to areas where such Classified Information is or may be developed, handled or stored, require a prior written authorization from the Competent Security Authority of the host Party receiving the visitors.

(2) Isäntäsopimuspuoli sallii vierailijoiden pääsyn turvallisuusluokiteltuun tietoon, sekä laitoksiin ja tiloihin, joissa harjoitetaan turvallisuusluokiteltuun tietoon liittyvää toimintaa tai säilytetään, tai käsitellään turvallisuusluokiteltua tietoa, ainoastaan jos

a. vieraat lähettävän sopimuspuolen toimivaltainen turvallisuusviranomainen tai muu toimivaltainen kyseisen valtion viranomainen on tehnyt vierailijoista turvallisuus selvityksen ja heillä on isäntäsopimuspuolen kansallisten lakien ja määräysten mukainen lupa ottaa vastaan turvallisuusluokiteltua tietoa; ja/tai

b. isäntäsopimuspuolen toimivaltainen turvallisuusviranomainen tai muu toimivaltainen kyseisen valtion viranomainen on antanut vierailijoille luvan tarvittavaan yhteen tai useampaan vierailuun.

(3) Vierailupyynnön esittävän sopimuspuolen toimivaltainen turvallisuusviranomainen ilmoittaa suunnitellusta vierailusta isäntäsopimuspuolen asianomaiselle toimivaltaiselle turvallisuusviranomaiselle tämän artiklan määräysten mukaisesti, sekä varmistaa, että isäntäsopimuspuolen toimivaltainen turvallisuusviranomainen saa vierailupyynnön vähintään kymmenen (10) työpäivää ennen vierailun ajankohtaa. Kiireellisissä tapauksissa toimivaltaiset turvallisuusviranomaiset voivat sopia lyhyemmästä ajasta.

(4) Vierailupyynnössä on oltava seuraavat tiedot:

a. vierailijan etu- ja sukunimi, syntymäaika ja -paikka sekä kansallisuus; vierailijan asema ja hänen edustamansa työnantaja; hanke, johon vierailija osallistuu; vierailijan passin tai muun henkilöllisyystodistuksen numero;

b. vahvistus vierailun tarkoitusta vastaavasta vierailijan turvallisuus selvityksestä;

c. vierailun tai vierailujen tarkoitus sekä maininta vierailuun liittyvän turvallisuusluokitellun tiedon korkeimmasta tasosta;

d. pyydetyn yhden tai useamman vierailun oletettu ajankohta ja kesto; toistuvien vierailujen osalta ilmoitetaan mahdollisuuksien mukaan ajanjakso, jolle vierailut ajoittuvat;

e. vierailun kohteena olevien laitoksen tai tilojen yhteyshenkilön nimi, osoite, puhelin- tai faksinumero ja sähköpostiosoite, tiedot ai-

(2) Access to Classified Information and to establishments and facilities where activities involving Classified Information are performed, or where Classified Information is stored or handled, shall be allowed by the host Party to visitors only if they have been:

a. security cleared by the Competent Security Authority or other competent government authority of the sending Party and are authorized to receive Classified Information in accordance with the national laws and regulations of the host Party, and/or

b. authorized by the Competent Security Authority or other competent government authority of the host Party to perform the required visit or visits.

(3) The Competent Security Authority of the requesting Party shall notify the relevant Competent Security Authority of the host Party of the planned visit in accordance with the provisions laid down in this Article, and shall make sure that the latter receives the visit request at least 10 working days before the visit takes place. In urgent cases the Competent Security Authorities may agree on a shorter period.

(4) The visit request shall include:

a. the visitor's surname, name, place and date of birth and nationality, the visitor's position, with a specification of the employer which the visitor represents, a specification of the project in which the visitor participates, the visitor's passport number or other identity document number;

b. confirmation of the visitor's Security Clearance in accordance with the purpose of the visit;

c. the purpose of the visit or visits, including the highest level of Classified Information to be involved;

d. the expected date and duration of the requested visit or visits. In the case of recurring visits the total period covered by the visits shall be stated, when possible;

e. the name, address, phone/fax number, e-mail and point of contact of the establishment/facility to be visited, previous contacts

emmista yhteyksistä sekä muut vierailun tai vierailujen aiheellisuuden määrittämiseksi tarpeelliset tiedot;

f. päiväys sekä vierailupyynnön lähettävän toimivaltaisen turvallisuusviranomaisen allekirjoitus tai leima.

(5) Vierailupyyntö toimitetaan noudattaen asianomaisten toimivaltaisten turvallisuusviranomaisten kesken sovittuja periaatteita.

(6) Toistuvia vierailuja koskevat luvat ovat voimassa enintään kaksitoista (12) kuukautta.

(7) Isäntäsopimuspuoli voi tarvittaessa pyytää todistusta turvallisuusselvityksestä.

(8) Muita vierailumenettelyjä voidaan soveltaa, jos asianomaisten sopimuspuolten toimivaltaiset turvallisuusviranomaiset sopivat siitä keskenään.

#### 8 artikla

##### *Turvallisuusluokitellut sopimukset*

(1) Ennen turvallisuusluokitellun sopimuksen tekemistä toisen sopimuspuolen maassa sopimuspuolen toimivaltainen turvallisuusviranomainen voi pyytää turvallisuusselvitystä (tai vastaavaa), jonka toisen sopimuspuolen toimivaltainen turvallisuusviranomainen on tehnyt kyseisen hankeosapuolen organisaatiosta. Jollei hankeosapuolesta ole tehty turvallisuusselvitystä, turvallisuusluokitellun sopimuksen tekevä sopimuspuoli voi pyytää hankeosapuolen edustamaa sopimuspuolta tekemään turvallisuusselvityksen (tai vastaavan) kansallisten lakien ja määräysten mukaisesti.

(2) Jos on kyse avoimesta tarjouskilpailusta, vastaanottavan sopimuspuolen toimivaltainen turvallisuusviranomainen voi antaa lähettävän sopimuspuolen toimivaltaiselle turvallisuusviranomaiselle asiaankuuluvat todistukset turvallisuusselvityksestä ilman virallista pyyntöä.

(3) Turvallisuusluokitellussa sopimuksessa on oltava asianmukaiset turvallisuusmääräykset, ja siihen on liitettävä asiakirjat, joissa määritetään kyseisessä sopimuksessa tarkoitettujen turvallisuusluokitellut tiedot tai sen turvallisuusluokitellut osat tai osatekijät.

(4) Turvallisuusluokitellun sopimuksen tekevän sopimuspuolen toimivaltainen turvallisuusviranomainen varmistaa, että sopimuksen toimeenpannaan toimivaltaiselle turvalli-

and any other information useful to determine the justification of the visit or visits;

f. the date and signature or stamp of the sending Competent Security Authority.

(5) The visit request shall be submitted in accordance with principles agreed upon by the relevant Competent Security Authorities.

(6) The validity of authorizations for recurring visits shall not exceed twelve (12) months.

(7) The host Party may, if necessary, request a Security Clearance Certificate.

(8) Other visit procedures may be used if mutually agreed between the Competent Security Authorities of the relevant Parties.

#### Article 8

##### *Classified Contracts*

(1) Prior to placing a Classified Contract within the country of any other Party, the Competent Security Authority of a Party may request a Security Clearance (or equivalent) issued to the facility of the Contractor in question by the Competent Security Authority of the other Party. If the Contractor does not possess a Security Clearance, the Party placing the Classified Contract may request the Party of the Contractor to issue a Security Clearance (or equivalent) in accordance with national laws and regulations.

(2) In the case of an open tender the Competent Security Authority of the Receiving Party may provide the Competent Security Authority of the Originating Party with the relevant security certificates without a formal request.

(3) A Classified Contract shall contain appropriate security provisions and be supplemented with documentation identifying the information or those elements or aspects of the Contract which are classified.

(4) The Competent Security Authority of the Party placing the Classified Contract shall ensure that copies of all relevant security documents in relation to the Contract are

suusviranomaiselle toimitetaan kopiot kaikista asianmukaisista sopimukseen liittyvistä turvallisuusasiakirjoista.

forwarded to the Competent Security Authority in whose country the Contract is to be implemented.

## 9 artikla

## Article 9

*Turvallisuusluokitellun tiedon kääntäminen, kopiointi ja hävittäminen**Translation, reproduction and destruction of Classified Information*

(1) Kaikkiin turvallisuusluokitellun tiedon kopioihin ja käännöksiin tehdään asianmukainen turvallisuusluokitusmerkintä, ja ne suojataan kuten alkuperäinen turvallisuusluokiteltu tieto. Käännöksiä ja kopioita tehdään ainoastaan viralliseen tarkoitukseen tarvittava vähimmäismäärä.

(1) All reproductions and translations shall bear appropriate security classification markings and be protected as the original Classified Information. The translations and the number of reproductions shall be limited to the minimum required for an official purpose.

(2) Kaikkiin käännöksiin tehdään asianmukainen käännöskielinen merkintä siitä, että käännökset sisältävät lähettävän sopimuspuolen turvallisuusluokiteltua tietoa.

(2) All translations shall contain a suitable annotation, in the language of translation, indicating that they contain Classified Information of the Originating Party.

(3) Merkinnällä TOP SECRET varustettua turvallisuusluokiteltua tietoa saa kääntää tai kopioida ainoastaan lähettävän sopimuspuolen kirjallisella luvalla.

(3) Classified Information marked TOP SECRET shall be translated or reproduced only upon the written permission of the Originating Party.

(4) Merkinnällä TOP SECRET varustettua turvallisuusluokiteltua tietoa ei hävitetä ilman lähettävän sopimuspuolen kirjallista ennakkosuostumusta. Se palautetaan lähettävälle sopimuspuolelle sen jälkeen, kun asianomaiset sopimuspuolet eivät enää katso sitä tarvittavan.

(4) Classified Information marked TOP SECRET shall not be destroyed without the prior written consent of the Originating Party. It shall be returned to the Originating Party after it is no longer considered necessary by the relevant Parties.

(5) Turvallisuusluokkaan SECRET tai sitä alempaan turvallisuusluokkaan kuuluva tieto hävitetään sen jälkeen, kun vastaanottava sopimuspuoli ei enää katso sitä tarvittavan, kansallisten lakien ja määräysten mukaisesti.

(5) Information classified as SECRET or below shall be destroyed after it is no longer considered necessary by the Receiving Party, in accordance with the national laws and regulations.

(6) Jos kriisitilanteen vuoksi on mahdotonta suojata tämän sopimuksen mukaisesti välitettyä turvallisuusluokiteltua tietoa, tämä tieto hävitetään välittömästi. Vastaanottava sopimuspuoli ilmoittaa turvallisuusluokitellun tiedon hävittämisestä mahdollisimman pian lähettävän sopimuspuolen toimivaltaiselle turvallisuusviranomaiselle.

(6) If a crisis situation makes it impossible to protect Classified Information transferred under this Agreement, the Classified Information shall be destroyed immediately. The Receiving Party shall notify the Competent Security Authority of the Originating Party about the destruction of the Classified Information as soon as possible.

## 10 artikla

## Article 10

*Turvallisuusluokitellun tiedon välittäminen**Transfer of Classified Information*

(1) Sopimuspuolet välittävät turvallisuusluokiteltua tietoa toisilleen pääsääntöisesti diplomaattiteitse tai kuriiritse, jolleivät asian-

(1) Classified Information shall normally be transferred between the Parties by using diplomatic channels or couriers, unless oth-

omaiset toimivaltaiset turvallisuusviranomaiset muuta sovi.

(2) Jos sopimuspuoli haluaa siirtää turvallisuusluokiteltua tietoa alueensa ulkopuolelle, siirrosta sovitaan ennakolta lähettävän sopimuspuolen kanssa.

#### 11 artikla

##### *Tietoturvaloukkaus*

(1) Jos todetaan tietoturvaloukkaus, jonka johdosta tässä sopimuksessa tarkoitettua turvallisuusluokiteltua tietoa katoaa tai ilmaistaan luvatta, sen maan toimivaltainen turvallisuusviranomainen, jossa tietoturvaloukkaus on tapahtunut, ilmoittaa asiasta mahdollisimman pian asianomaisten sopimuspuolten toimivaltaisille turvallisuusviranomaisille.

(2) Toimivaltainen sopimuspuoli toteuttaa kaikki asianmukaiset kansallisen lainsäädäntönsä mahdollistamat toimet rajoittaakseen tietoturvaloukkauksen seurauksia ja estääkseen tietoturvan muun loukkaamisen tai vaarantumisen.

(3) Muut asianomaiset sopimuspuolet antavat pyynnöstä toisilleen tutkinta-apua. Muille asianomaisille sopimuspuolille ilmoitetaan joka tapauksessa tutkinnan tuloksista ja toimista, jotka tietoturvaloukkauksen johdosta on toteutettu, ja niille toimitetaan loppulausunto tietoturvaloukkauksen syistä ja laajuudesta sekä toimista, jotka on toteutettu tietoturvaloukkauksen uusimisen estämiseksi.

#### 12 artikla

##### *Kustannukset*

Sopimuspuolet eivät korvaa toisilleen niille tästä sopimuksesta aiheutuneita kustannuksia.

#### 13 artikla

##### *Riitojen ratkaiseminen*

Kaikki tämän sopimuksen tulkintaan tai soveltamiseen liittyvät riidat ratkaistaan sopimuspuolten välisin neuvotteluin, eikä niitä saateta kansallisen tai kansainvälisen tuomioistuimen tai kolmannen osapuolen ratkaistaviksi.

erwise agreed by the relevant Competent Security Authorities.

(2) If one of the Parties wishes to transfer Classified Information outside its territory, such transfer shall be subject to prior coordination with the Originating Party.

#### Article 11

##### *Breach of Security*

(1) In case of a Breach of Security involving loss or unauthorized disclosure of Classified Information under this Agreement, the Competent Security Authority in whose country the Breach of Security occurs shall inform the Competent Security Authorities of the Parties concerned as soon as possible.

(2) The Party with jurisdiction shall undertake all appropriate measures possible under its national law so as to limit the consequences of the Breach of Security and to prevent further breaches or compromises.

(3) Upon request, the other Parties concerned shall provide investigative assistance. In any case, the other Parties concerned shall be informed of the results of the investigation and of the measures undertaken as a result of the Breach of Security, and shall receive a final statement as to the reasons and extent of the Breach of Security, and the measures adopted to prevent reoccurrences.

#### Article 12

##### *Expenses*

Expenses incurred by the Parties with respect to this Agreement shall not be subject to reimbursement between the Parties.

#### Article 13

##### *Dispute settlement*

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

## 14 artikla

*Loppumääräykset*

(1) Tämä sopimus on ratifioitava tai hyväksyttävä. Ratifioimis- tai hyväksymiskirjat talletetaan tallettajaksi nimettävän Norjan kuningaskunnan hallituksen huostaan.

(2) Tämä sopimus tulee voimaan kolmantenakymmenentenä (30) päivänä siitä päivästä, jona viimeinen allekirjoittajahallitus on tallettanut ratifioimis- tai hyväksymiskirjansa.

(3) Tämän sopimuksen voimaantuloon saakka sopimuspuoli voi ilmoittaa ratifioimis- tai hyväksymiskirjaansa tallettaessaan tai myöhemmin, että se katsoo sopimuksen sitovan sitä sen suhteissa muuhun sopimuspuoleen, joka on tehnyt samanlaisen ilmoituksen. Ilmoitukset tulevat voimaan kolmantenakymmenentenä (30) päivänä siitä päivästä, jona ne on vastaanotettu.

(4) Tätä sopimusta voidaan muuttaa kirjallisesti milloin tahansa kaikkien sopimuspuolten suostumuksella.

(5) Tämän artiklan 4 kappaleen mukaisesti hyväksytty muutos tulee voimaan kolmantenakymmenentenä (30) päivänä siitä päivästä, jona viimeinen sopimuspuoli on ilmoittanut tallettajalle hyväksyneensä muutoksen.

(6) Tämän sopimuksen tultua voimaan se on avoinna liittymistä varten kolmansille valtioille allekirjoittajahallitusten suostumuksella. Liittymiskirjat talletetaan Norjan kuningaskunnan hallituksen huostaan.

(7) Sopimukseen liittyvän valtion osalta sopimus tulee voimaan kolmantenakymmenentenä (30) päivänä siitä päivästä, jona tämä valtio on tallettanut liittymiskirjansa.

(8) Tämä sopimus on voimassa toistaiseksi. Sopimuspuoli voi milloin tahansa irtisanoa sopimuksen ilmoittamalla siitä kirjallisesti tallettajalle. Irtisanominen tulee voimaan irtisanoutuvan sopimuspuolen osalta kuuden (6) kuukauden kuluttua irtisanomisilmoituksen tallettamisesta.

(9) Jos tämä sopimus sanotaan irti, sopimuksen määräysten mukaisesti välitetty tur-

## Article 14

*Final provisions*

(1) This Agreement is subject to ratification, acceptance or approval. The instruments of ratification, acceptance or approval shall be deposited with the Government of the Kingdom of Norway, which is hereby designated as the Depositary.

(2) This Agreement shall enter into force on the thirtieth (30) day following the date of deposit of the instruments of ratification, acceptance or approval by the last signatory Government.

(3) Until the entry into force of this Agreement, each Party may notify at the time of the deposit of the instrument of ratification, acceptance or approval, or at any other subsequent time, that it shall consider itself bound by the Agreement in its relations with any other Party having made the same notification. These notifications shall take effect thirty (30) days after the date of receipt of the notification.

(4) Amendments to this Agreement may be made in writing at any time with the consent of all the Parties.

(5) Any amendment adopted in accordance with Paragraph 4 shall enter into force on the thirtieth (30) day after the last Party has informed the Depositary of its acceptance of the amendment.

(6) After the entry into force of this Agreement it shall be open to accession by third states upon consent of the signatory Governments. The instruments of accession shall be deposited with the Government of the Kingdom of Norway.

(7) For each acceding State this Agreement shall enter into force on the thirtieth (30) day following the date of deposit by such State of its instruments of accession.

(8) This Agreement shall be in force for an unlimited period of time. Any Party may, at any time, denounce the Agreement by means of a written notification to the Depositary. Such denunciation shall take effect with respect to the denouncing Party six (6) months after the date of deposit of the notification of denunciation.

(9) In the event of denunciation, Classified Information and/or items transmitted under

vallisuusluokiteltu tieto ja/tai aineisto palautetaan mahdollisimman pian lähetettävälle sopimuspuolelle. Palauttamattoman turvallisuusluokitellun tiedon tai aineiston suojaamista jatketaan tämän sopimuksen määräysten mukaisesti.

(10) Tullessaan voimaan tämä sopimus korvaa seuraavat sopimuspuolten väliset sopimukset ja järjestelyt turvallisuusluokitellun tiedon suojaamiseksi:

1. ”Overenskomst mellom Kongeriket Sveriges regjering og Kongeriket Norges regjering vedrørende utveksling av militære informasjoner og materiell”/”Överenskommelse mellan Konungariket Sveriges regering och Konungariket Norges regering rörande visst utbyte av militära informationer och materiel”. Stockholm den 19 mai/maj 1969,

2. ”Sikkerhetsaftale. Overenskomst vedrørende sikkerhedsaftalens udformning inden for rammeaftalen omfattende nordisk samarbejde inden for forsvarsmaterielområdet mellem Danmark, Finland, Norge og Sverige”/”Turvallisuussuojasopimus. Pohjoismaisen puolustusmateriaalialan yhteistyösopimuksen puitteissa laadittu turvallisuussuojaa koskeva yhteisymmärrys Tanskan, Suomen, Norjan ja Ruotsin välillä”/”Sikkerhetsavtale. Overenskomst om sikkerhetstiltakenes utforming innenfor rammen av avtalen om nordisk samarbeid på forsvarsmateriellområdet mellom Danmark, Finland, Norge og Sverige”/”Säkerhetsskyddsavtal. Överenskommelse rörande säkerhetsskyddets utformning inom ramen för avtalet om nordisk samarbete inom försvarsmaterielområdet mellan Danmark, Finland, Norge och Sverige“. 1994/1995.

Näiden sopimusten ja järjestelyjen mukaisesti vaihdetun turvallisuusluokitellun tiedon suojaamista jatketaan tämän sopimuksen määräysten mukaisesti.

Tämä sopimus on tehty yhtenä englannin-, tanskan-, suomen-, islannin-, norjan- ja ruotsinkielisenä alkuperäiskappaleena. Jos syntyy tulkintaeroja, englanninkielinen teksti on ratkaiseva. Allekirjoitettu sopimus talletetaan Norjan kuningaskunnan ulkoasiainministeriön arkistoon. Norjan kuningaskunnan ulkoasiainministeriö toimittaa oikeaksi todistetut jäljennökset sopimuksesta kaikille sopimuspuolille.

the terms of this Agreement shall be returned to the Originating Party as soon as possible. Classified Information and/or items that are not returned shall continue to be protected in accordance with the provisions of this Agreement.

(10) When entering into force, this Agreement replaces the following Agreements and Arrangements concerning the protection of Classified Information between the Parties:

1. ”Overenskomst mellom Kongeriket Sveriges regjering og Kongeriket Norges regjering vedrørende utveksling av militære informasjoner og materiell”/”Överenskommelse mellan Konungariket Sveriges regering och Konungariket Norges regering rörande visst utbyte av militära informationer och materiel”. Stockholm den 19 mai/maj 1969,

2. ”Sikkerhetsaftale. Overenskomst vedrørende sikkerhedsaftalens udformning inden for rammeaftalen omfattende nordisk samarbejde inden for forsvarsmaterielområdet mellem Danmark, Finland, Norge og Sverige”/”Turvallisuussuojasopimus. Pohjoismaisen puolustusmateriaalialan yhteistyösopimuksen puitteissa laadittu turvallisuussuojaa koskeva yhteisymmärrys Tanskan, Suomen, Norjan ja Ruotsin välillä”/”Sikkerhetsavtale. Overenskomst om sikkerhetstiltakenes utforming innenfor rammen av avtalen om nordisk samarbeid på forsvarsmateriellområdet mellom Danmark, Finland, Norge og Sverige”/”Säkerhetsskyddsavtal. Överenskommelse rörande säkerhetsskyddets utformning inom ramen för avtalet om nordisk samarbete inom försvarsmaterielområdet mellan Danmark, Finland, Norge och Sverige“. 1994/1995.

Classified Information exchanged under the above-mentioned Agreements and Arrangements shall continue to be protected in accordance with the terms of this Agreement.

This Agreement is produced in a single copy in the English, Danish, Finnish, Icelandic, Norwegian and Swedish languages. In case of differences of interpretation, the English text shall prevail. The signed copy of this Agreement shall be deposited in the archives of the Ministry of Foreign Affairs of the Kingdom of Norway. The Ministry of Foreign Affairs of the Kingdom of Norway shall transmit certified copies to all the Parties.



Tämän vakuudeksi asianmukaisesti valtuutetut hallitustensa edustajat ovat allekirjoittaneet tämän sopimuksen. Tehty Osllossa 7 päivänä toukokuuta 2010.

Tanskan kuningaskunnan  
hallituksen puolesta

Suomen tasavallan  
hallituksen puolesta

Islannin hallituksen puolesta

Norjan kuningaskunnan  
hallituksen puolesta

Ruotsin kuningaskunnan  
hallituksen puolesta

In witness whereof the duly authorised representatives of their respective Governments have signed this Agreement. Done in Oslo, this 7 day of May, two thousand and ten.

On behalf of the Government of the  
Kingdom of Denmark

On behalf of the Government of the  
Republic of Finland

On behalf of the Government of Iceland

On behalf of the Government of the  
Kingdom of Norway

On behalf of the Government of the  
Kingdom of Sweden