Hallituksen esitys eduskunnalle turvallisuusluokitellun tiedon vastavuoroisesta suojaamisesta Suomen ja Sveitsin välillä tehdyn sopimuksen hyväksymisestä sekä laiksi mainitun sopimuksen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta

ESITYKSEN PÄÄASIALLINEN SISÄLTÖ

Esityksessä ehdotetaan, että eduskunta hyväksyisi Suomen ja Sveitsin välisen sopimuksen turvallisuusluokitellun tiedon vastavuoroisesta suojaamisesta sekä lain sopimuksen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta.

Sopimuksen tarkoituksena on varmistaa salassa pidettävän turvallisuusluokitellun tiedon suojaaminen Suomen ja Sveitsin välillä osapuolten välisessä yhteistyössä erityisesti ulko-, puolustus-, turvallisuus-, tiede- tai yritysasioissa sekä teknisissä asioissa. Kysymys on arkaluonteisista tietoaineistoista, jotka lähettävässä sopimusvaltiossa on erikseen luokiteltu korkean tietoturvallisuuden tason toteuttamista edellyttäviksi. Sopimus ei velvoita turvallisuusluokitellun tiedon vaihtamiseen.

Sopimus tulee voimaan, kun jälkimmäinen ilmoitus siitä, että sopimuksen voimaansaattamiseksi tarvittavat kansalliset toimenpiteet on saatettu loppuun, on otettu vastaan. Sopimuksen voimaansaattamislaki on tarkoitettu tulemaan voimaan valtioneuvoston asetuksella säädettävänä ajankohtana samaan aikaan kuin sopimus tulee Suomen osalta voimaan.

SISÄLLYS

YLEISPERUSTELUT

1 Johdanto

Tietoturvallisuudella tarkoitetaan 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 sovittuun tarkoitukseen sekä erilaiset tietojen käsittelyyn ja siirtoon liittyvät menettelytapavaatimukset. Tietoturvallisuusvaatimukset kattavat informaation koko elinkaaren sisältäen tietojen hankkimisen, muokkaamisen, käytön, luovutuksen, arkistoinnin ja hävittämisen.

Kansainväliseen yhteistyöhön liittyviin asiakirjoihin sisältyy toisinaan sellaisia 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 puolustushallintojen väliseen yhteistyöhön liittyvän ei-julkisen tiedonvaihdon suojaamisen. Välittömän valtiovastuun piiriin kuuluvien kysymysten lisäksi kansainvälisillä tietoturvallisuusvelvoitteilla on kuitenkin kasvava merkitys myös taloudellisen, teollisen ja teknologisen yhteistyön kannalta, joiden puitteissa yhä useammat yritystason hankkeet edellyttävät turvallisuusluokitellun tiedon hyödyntämistä. Näin 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 nykyään yhä enenevässä määrin myös muilla sektoreilla tapahtuvat hankinnat, kuten esimerkiksi informaatioteknologian ja ydinvoima-alan hankinnat.

Pyrkimyksistä huolimatta ei kuitenkaan 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. Edellä sanotusta poikkeuksena on kuitenkin Tanskan, Suomen, Islannin, Norjan ja Ruotsin välillä turvallisuusluokitellun tiedon vastavuoroisesta suojaamisesta ja vaihtamisesta tehty yleinen turvallisuussopimus (SopS 11 ja 12/2013).

Yleissopimuksen puuttuminen on pakottanut 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) jäsen on Suomelle tärkeä yhteistyökumppani niin turvallisuushallinnon kuin taloudellisen vuorovaikutuksenkin 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 jäsenmaiden kanssa ESA:n turvallisuusluokiteltuihin tarjouskilpailuihin. Tietoturvallisuussopimus on tehty myös Länsi-Euroopan unionin (WEU) kanssa (SopS 41 ja 42/1998) ja Eurooppalaisen puolustusmateriaaliyhteistyöjärjestön (OCCAR) (SopS 109 ja 110/2008) ja Pohjois-Atlantin liiton (Nato) (SopS 7 ja 8/2013) kanssa. 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), Espanjan (SopS 38 ja 39/2010), Amerikan yhdysvaltojen (SopS 41 ja 42/2013), Iso-Britannian (SopS 49 ja 50/2013) ja Luxemburgin (SopS 59 ja 60/2013) kanssa. Suomi on 10 päivänä toukokuuta 2012 hyväksynyt EU:n jäsenvaltioiden välillä toukokuussa 2011 allekirjoitetun sopimuksen turvallisuusluokitellun tiedon suojaamisesta. Lisäksi Suomi on tehnyt soveltamisalaltaan suppeamman tietoturvallisuussopimuksen Israelin kanssa puolustus- tai turvallisuushallintojen kesken välitetystä turvallisuusluokitellusta tiedosta (SopS 34 ja 35/2012).

Tietoturvallisuussopimuksella luodaan edellytykset turvallisuusluokitellun tiedon vaihtamiseen osapuolten välillä. Sopimuksella varmistutaan siitä, että Suomen luovuttama turvallisuusluokiteltu tieto pidetään vastaanottajamaassa salassa ja sitä suojataan ja käsitellään asianmukaisesti. Tietoturvallisuussopimuksen avulla myös toinen osapuoli voi varmistua siitä, että Suomi suojaa ja käsittelee sen luovuttamaa turvallisuusluokiteltua tietoa asianmukaisesti.

2 Nykytila

2.1 Laki kansainvälisistä tietoturvallisuusvelvoitteista

Lain yleinen soveltamisala

Laki kansainvälisistä tietoturvallisuusvelvoitteista (588/2004) säädettiin osana Suomen ja Saksan välisen tietoturvallisuussopimuksen sekä ESA:n tietoturvallisuussopimuksen voimaansaattamista. Laki katsottiin tarpeelliseksi muun ohella sen vuoksi, että kansainvälisten sopimusten panemiseksi täytäntöön on tarve poiketa asiakirjajulkisuuteen ja -turvallisuuteen perustuvista kansallisista järjestelyistä, jotka perustuvat pääosin viranomaisten toiminnan julkisudesta annettuun lakiin (621/1999), jäljempänä *julkisuuslaki*.

Lakia kansainvälisistä tietoturvallisuusvelvoitteista sovelletaan erityissuojattaviin tietoaineistoihin. Näillä tarkoitetaan salassa pidettäviä asiakirjoja ja materiaaleja, jotka on toimitettu Suomen viranomaiselle ja joiden luovuttaja on kansainvälisen, Suomea sitovan sopimuksen tai muun kansainvälisen velvoitteen mukaisesti tehnyt niihin turvallisuusluokkaa koskevan merkinnän. Määräysvalta luovutettuun tietoon säilyy luovutuksen jälkeenkin aineiston luovuttaneella valtiolla. 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 tietoaineistoja 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 erityissuojattavan tietoaineiston pohjalta. Lakia ei sovelleta pelkästään Suomen kansallista tietoa sisältävien asiakirjojen tai niiden osien salassapitoon tai luokitukseen.

Laissa säädettyjä 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 tietoturvallisuusvelvoitteista annettuun lakiin sisältyy kansallisten asiakirjojen tietoturvallisuudesta annetuista säännöksistä poikkeavia säännöksiä. Laissa on kuitenkin yleinen viittaussäännös julkisuuslakiin. Niiltä osin kuin suomalaisten viranomaisten asiakirjoihin sisältyy muita kuin kansainvälisten tietoturvallisuusvelvoitteiden piiriin kuuluvia tietoja kansainvälisestä yhteistyöstä, on sovellettava julkisuuslain ja sen nojalla annettuja säännöksiä. Laissa on myös erityissäännös, joka koskee päätöksentekovaltaa siinä tilanteessa, että 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 ratkais-

tavaksi julkisuuslain 15 §:ssä säädetyissä tilanteissa.

Lain soveltaminen elinkeinonharjoittajiin

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

Turvallisuusluokitellulla sopimuksella tarkoitetaan sopimusta, jonka toisen valtion viranomainen tai siinä kotipaikkaansa pitävä yritys taikka kansainvälinen järjestö tai toimielin aikoo tehdä tai on tehnyt kansainvälisessä tietoturvallisuusvelvoitteessa tarkoitetulla tavalla Suomessa kotipaikkaansa pitävän elinkeinonharjoittajan kanssa, jos tarjouskilpailuun osallistuminen tai sopimuksen toteuttaminen voi edellyttää pääsyä erityissuojattavaan tietoaineistoon (2 §:n 3 kohta).

Elinkeinonharjoittaja voi pyytää yhteisöturvallisuusselvityksen ja arvion tekemistä voidakseen osallistua toisen valtion viranomaisen tai siinä kotipaikkaansa pitävän yrityksen järjestämään tarjouskilpailuun (12 §:n 2 mom.). Säännöksen tarkoituksena on turvata suomalaisten yritysten kilpailumahdollisuudet hankinnoissa silloinkin, kun hankintaan sovellettavissa olevaa kansainvälistä tietoturvallisuussopimusta ei ole. Useimmat valtiot kuitenkin edellyttävät kahdenvälisen tietoturvallisuussopimuksen olemassa oloa ulkomaisen turvallisuustodistuksen hyväksymiseksi.

Elinkeinonharjoittajalla ja tämän palveluksessa tai toimeksiannosta toimivalla on erityissuojattavia tietoaineistoja koskeva salassapitovelvollisuus (6 §). Elinkeinonharjoittajalla on myös velvollisuus kansainvälisten tietoturvallisuusvelvoitteiden toteuttamiseksi antaa toimivaltaiselle turvallisuusviranomaiselle tietoja sekä sallia viranomaisen ja kansainvälisen toimielimen tai sopimusvaltion edustajan tutustuminen turvallisuusjärjestelyihinsä ja toimitiloihinsa (16 §:n 2 mom. ja 18 §:n 2 mom.).

Lain täytäntöönpanoviranomaiset

Laissa on säännökset (4 §) niistä viranomaisista, jotka huolehtivat kansainvälisten tietoturvallisuusvelvoitteiden hoitamisesta. Kansallisena turvallisuusviranomaisena (*National Security Authority, NSA*) kansainvälisten tietoturvallisuusvelvoitteiden toteuttamiseen liittyvissä tehtävissä toimii ulkoasiainministeriö. Puolustusministeriö, pääesikunta, Suojelupoliisi ja Viestintävirasto toimivat määrättyinä turvallisuusviranomaisina (*Designated Security Authority, DSA*). Näille viranomaisille voi kuulua muun ohella tarjous- ja hankintamenettelyihin liittyvien asiakirjojen turvallisuusluokittelu.

Henkilöturvallisuutta koskevien turvallisuusselvitysten, jäljempänä henkilöturvallisuusselvitys, laadinnasta huolehtivat Suojelupoliisi ja pääesikunta (11 §). Yhteisöturvallisuusselvityksen laadinta kuuluu lain mukaan Suojelupoliisille, paitsi silloin, kun kyse on puolustukseen liittyvästä hankinnasta, jolloin selvitysten tekemisestä huolehtii pääesikunta (12 §). Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 5 §:n 2 momentin mukaan kansallinen turvallisuusviranomainen ja tehtävään määrätyt turvallisuusviranomaiset voivat sen estämättä, mitä muun muassa toimivallasta yhteisöturvallisuusselvitysten laadinnasta säädetään, sopia tietyn tehtävän tai tehtäväkokonaisuuden hoitamisesta toisen turvallisuusviranomaisen lukuun, jos järjestely on tarpeen tehtävien hoitamiseksi tarkoituksenmukaisesti, taloudellisesti ja joutuisasti. Viestintävirasto on lain 4 §:n 1 momentissa (885/2010) määrätty turvallisuusviranomaiseksi, jonka tehtävänä on toimia asiantuntijana tietojärjestelmien ja tietoliikennejärjestelyjen turvallisuutta koskevissa asioissa.

Laissa kansainvälisistä tietoturvallisuusvelvoitteista on säännökset viranomaisia ja elinkeinonharjoittajaa koskevasta tiedonantovelvollisuudesta (16 §). Säännösten tarkoituksena on varmistaa, että toimivaltaiset turvallisuusviranomaiset voisivat saada niille kuuluvien tehtävien hoitamiseksi tarpeelliset tiedot. Viranomaiset voivat myös salassapitovelvollisuuden estämättä antaa kansainväliseen tietoturvallisuusvelvoitteeseen perustuvaa yhteistyötä varten salassa pidettäviä tietoja ulkomaiselle sopimuspuolelle (17 §). Vi-

ranomaisella on myös oikeus sallia kansainväliseen tietoturvallisuusvelvoitteeseen perustuva kansainvälisen järjestön, toimielimen tai sopimusvaltion edustajan tutustuminen viranomaisen toteuttamiin turvallisuusjärjestelyihin ja toimitiloihin riippumatta siitä, mitä turvallisuusjärjestelyjen salassapidosta säädetään taikka säädetään tai määrätään pääsystä tiloihin, joissa käsitellään tai säilytetään salassa pidettäviä tietoja (18 §).

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

Tietojen salassapito ja käytön sääntely

Erityissuojattava tietoaineisto on pidettävä salassa, jollei kansainvälisestä tietoturvallisuusvelvoitteesta muuta johdu (6 §:n 1 mom.). Salassapitovelvollisuus koskee myös elinkeinonharjoittajaa tämän ollessa osapuolena turvallisuusluokitellussa sopimuksissa. Suomen tekemissä, käytännössä kahdenvälisissä sopimuksissa, jotka koskevat eri maiden viranomaisten välistä salassa pidettävien tietojen vaihtoa, on säännönmukaisesti määräys, joka rajoittaa luovutettujen tietojen käyttöä. Kyseisen määräyksen 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. Erityissuojattavien tietoaineistojen käyttöä koskee siten vahva käyttötarkoitussidonnaisuus.

Turvallisuusluokittelu ja –toimenpiteet

Laissa säädetään velvollisuudesta merkitä erityissuojattavaan tietoaineistoon sen turvallisuusluokka. Tietoaineistoon tehty merkintä turvallisuusluokasta osoittaa, minkälaisia toimenpiteitä on toteutettava aineistoa käsiteltäessä (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 eri turvallisuusluokkia vastaavista 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.

Turvallisuusluokiteltuja tietoja viranomaisissa käytettäessä on noudatettava pidättyvyyttä ja sen vuoksi lakiin kansainvälisistä tietoturvallisuusvelvoitteista on kirjattu kansainvälisissä sopimuksissa oleva yleinen vaatimus siitä, 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 §:n 3 mom.).

Henkilöstöturvallisuus

Kansainvälisessä tietoturvallisuusvelvoitteessa edellytetty henkilöturvallisuussuusselvitys tehdään siten kuin turvallisuusselvityksistä annetussa laissa (177/2002) ja sen nojalla säädetään. Siten esimerkiksi selvityksen kohteena olevan henkilön oikeudet määräytyvät sanotun lain mukaisesti.

Kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa on kuitenkin kaksi säännöstä, jotka ovat erityissäännöksiä suhteessa turvallisuusselvityksistä annettuun lakiin. Suppea turvallisuusselvitys on mahdollista laatia muissakin kuin turvallisuusselvityksistä annetun lain 19 §:ssä luetelluissa tapauksissa, jos se on tarpeen kansainvälisen tietoturvallisuusvelvoitteen toteuttamiseksi (11 §:n 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 §:n 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 säädetty henkilön luotettavuuden arvioinnista. Tällaisen arvion tekee turvallisuusselvityksen perusteella kansallinen turvallisuusviranomainen tai, jos turvallisuusviranomaisten välillä on niin sovittu, tehtävään määrätty turvallisuusviranomainen (11 §:n 3 mom.).

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

Yhteisöturvallisuusselvitys

Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 12 §:ssä säädetään yhteisöturvallisuusselvityksistä ja arvioista. Yhteisöturvallisuusselvityksellä varmistetaan elinkeinonharjoittajan toimitilojen ja käsittelykäytäntöjen asianmukaisuus sekä henkilöstön osaaminen. Elinkeinonharjoittajan luotettavuuden arvioinnilla varmistutaan 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 Suojelupoliisi. Pääesikunta huolehtii tehtävästä kuitenkin silloin, kun kysymys on puolustukseen liittyvästä hankinnasta. Selvitystä laadittaessa on otettava huomioon laissa yksilöidyt seikat, muun muassa se, miten suojataan turvallisuusluokiteltuja tietoja oikeudettomalta ilmitulolta, muuttamiselta ja hävittämiseltä, ja miten estetään asiaton pääsy tiloihin, joissa turvallisuusluokiteltuja tietoja käsitellään tai joissa harjoitetaan turvallisuusluokitellussa sopimuksessa tarkoitettua toimintaa. Viestintävirasto laatii tarvittaessa osana yhteisöturvallisuusselvitystä selvityksen ja arvion siitä, täyttävätkö elinkeinonharjoittajan tietojärjestelmät ja tietoliikenteen järjestelyt kansainvälisistä tietoturvallisuusvelvoitteista johtuvat vaatimukset.

Määrätyt turvallisuusviranomaiset voivat toimialaansa kuuluvaa yhteisöturvallisuusselvitystä ja sen perusteella annettavaa arviota laatiessaan lain 13 §:n mukaan edellyttää, että elinkeinonharjoittaja sitoutuu huolehtimaan 12 §:n 1 momentissa tarkoitetuista ja muista kansainvälisten tietoturvallisuusvelvoitteiden toteuttamiseksi tarpeellisista toimenpiteistä. Sitoumuksessa voidaan yksityiskohtaisemmin määritellä ne toimenpiteet, jotka elinkeinonharjoittaja toteuttaa täyttääkseen kansainvälisistä tietoturvallisuusvelvoitteista johtuvat vaatimukset. Sitoumuksessa elinkeinonharjoittaja sitoutuu myös tekemään ne mahdolliset tarkistukset toimintaansa, jotka toiminnan turvallisuuskartoituksessa on havaittu. Turvallisuusselvityksen ja mahdollisen sitoumuksen jälkeen Suojelupoliisi tai pääesikunta voi tehdä arvion elinkeinonharjoittajan luotettavuudesta ja antaa tätä koskevan turvallisuustodistuksen (Facility Security Clearance Certificate).

2.2 Turvallisuusselvityksiä koskeva lainsäädäntö

Henkilöturvallisuusselvityksistä 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. Turvallisuus-

selvitys tehdään laissa määritellyissä tapauksissa, kuten silloin, kun Suomea sitova valtiosopimus tai muu kansainvälinen velvoite edellyttää turvallisuusselvityksen tekemistä tai sen perusteella laaditun todistuksen esittämistä.

Yksityisyyden suojan perusoikeusluonteen vuoksi turvallisuusselvitysmenettely on tarkan muotosidonnaista. Turvallisuusselvitys voidaan tehdä vain selvityksen kohteena olevan henkilön etukäteen antaman, nimenomaisen ja kirjallisen suostumuksen perusteella. Myös turvallisuusselvitysmenettelyssä käytettävät rekisterit on laissa lueteltu tyhjentävästi.

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

Oikeusministeriö asetti turvallisuusselvityslain kokonaistarkistusta varten työryhmän, joka luovutti mietintönsä oikeusministerille 31 päivänä tammikuuta 2011. Työryhmän tehtävänä oli turvallisuusselvityslain kehittäminen siten, että se vastaa Suomea sitovia velvoitteita ja kansainvälisesti yleisesti sovellettavia käytäntöjä. Hallituksen esitys eduskunnalle turvallisuusselvityslaiksi ja eräiksi siihen liittyviksi laeiksi (HE 57/2013 vp) annettiin eduskunnalle kevätistuntokaudella ja esityksen käsittely on kesken. Turvallisuusselvityslakia koskevalla esityksellä ei hyväksytyksi tullessaan ole vaikutusta nyt hyväksyttäväksi esitettyihin sopimusmääräyksiin.

3 Esityksen tavoitteet ja keskeiset ehdotukset

Esityksen tavoitteena on saattaa voimaan Suomen ja Sveitsin välinen tietoturvallisuussopimus ja näin varmistua siitä, että Suomen Sveitsiin luovuttamaa turvallisuusluokiteltua tietoa suojataan ja käsitellään asianmukaisesti. Esityksen tavoitteena on myös edistää Suomen mahdollisuuksia vastaanottaa Sveitsin turvallisuusluokiteltua tietoa ja parantaa maiden välistä yhteistyötä tietoturvallisuuden alalla. Lisäksi esityksen tarkoituksena on turvata suomalaisten yritysten mahdollisuudet osallistua sellaisiin kansainvälisiin sekä Suomen ja Sveitsin välisiin hankkeisiin, joiden toteuttaminen saattaa edellyttää turvallisuusluokiteltujen tietojen vaihtoa ja parantaa näin suomalaisten yritysten kilpailukykyä.

4 Esityksen vaikutukset

4.1 Vaikutukset kansalaisiin

Sopimuksen voimaansaattamisen myötä Sveitsistä Suomeen toimitettuihin turvallisuusluokiteltuihin tietoihin ja materiaaleihin (erityissuojattava tietoaineisto) sovellettaisiin lakia kansainvälisistä tietoturvallisuusvelvoitteista. Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain mukainen erityissuojattavan tietoaineiston suojaaminen perustuu sopimuksen määräyksiin.

Suomen ja Sveitsin välisen sopimuksen mukaisia erityissuojattavia tietoaineistoja ovat aineistot, joita Sveitsi pitää salassa pidettävinä ja jotka se on määritellyt ja merkinnyt korkean tietoturvallisuuden tasoa edellyttäviksi. Sopimuksen 5 artiklassa määrätään turvallisuusluokitellun tiedon salassapidosta. Artiklan 2 kohdan mukaan osapuolet eivät salli kolmansille osapuolille pääsyä turvallisuusluokiteltuun tietoon ilman luovuttavan osapuolen kirjallista ennakkosuostumusta. Tämä merkitsee poikkeusta julkisuuslain yleistä etua koskevista salassapitosäännöksistä, joissa salassapito on useimmissa tapauksissa riippuvainen siitä, minkälaisia vaikutuksia tietojen antamisella olisi suojattavalle edulle. Ilman tietoturvallisuussopimustakin Sveitsin Suomeen luovuttamat turvallisuusluokitellut asiakirjat pidettäisiin säännönmukaisesti salassa kansainvälisiä suhteita koskevina julkisuuslain 24 §:n 1 momentin 2 kohdan perusteella, mikä merkitsee, että tietoturvallisuussopimus ei rajoita kansalaisen tiedonsaantia enempää kuin mitä se julkisuuslain mukaan on.

Merkittävimpänä erona on se, että viranomaisella ei olisi kansainvälisessä tietoturvallisuusvelvoitteessa tarkoitettuun asiakirjaan kohdistuvaa tiedonsaantipyyntöä ratkaistessaan velvollisuutta erikseen perustella tiedon antamisesta aiheutuvaa vahinkoa. Tiedonsaantipyyntö olisi muutoin käsiteltävä julkisuuslain mukaisesti. Jos syntyy epäsel-

vyyttä luokituksen oikeellisuudesta tai siitä, mitkä asiakirjassa olevat tiedot ovat johtaneet luokitusmerkintään, viranomaisen on otettava yhteyttä asiakirjan laatineeseen osapuoleen.

Suomen ja Sveitsin välinen tietoturvallisuussopimus ei vaikuta Suomen kansallisten asiakirjojen salassapitoon tai luokitukseen, mitkä määräytyvät julkisuuslain mukaan.

Henkilöstöturvallisuus on keskeinen tietoturvallisuuden osa-alue. Koska jo laki kansainvälisistä tietoturvavelvoitteista edellyttää turvallisuusselvityksistä annetun lain mukaisen menettelyn käyttämistä henkilöstön luotettavuuden varmistamisessa, ehdotetun voimaansaattamislain hyväksyminen ei tarkoittaisi sitä, että kansalaisten yksityisyyselämän ja henkilötietojen suojaa kavennettaisiin aikaisempaan verrattuna.

4.2 Vaikutukset elinkeinoelämään

Sopimus antaa suomalaisille yrityksille mahdollisuuden saada sellaisia tilauksia tai osallistua sellaisiin hankkeisiin, joiden toteuttaminen edellyttää pääsyä Sveitsin turvallisuusluokiteltuihin tietoihin. Vastaavasti sopimus antaa sveitsiläisille yrityksille mahdollisuuden saada sellaisia tilauksia tai osallistua sellaisiin hankkeisiin, joiden toteuttaminen edellyttää pääsyä Suomen turvallisuusluokiteltuun tietoon. Tulevien hankkeiden määrää ja taloudellista arvoa on etukäteen vaikea arvioida. Turvallisuusluokiteltua tietoa sisältäviä hankkeita toteutetaan erityisesti puolustusteollisuuden, turvallisuuden, ydinvoiman, informaatioteknologian ja muun korkean teknologian aloilla sekä tieteen- ja tutkimuksen aloilla. Ilman tietoturvallisuussopimusta suomalaiset yritykset voisivat jäädä Sveitsissä toteutettavien hankkeiden ulkopuolelle. Sopimuksen tarkoituksena onkin luoda tarvittavat järjestelyt ja menettelyt ennakkoon, jotta hankkeisiin osallistuminen olisi mahdollista ja näin parantaa suomalaisten yritysten kilpailukykyä.

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. Sopimus lisää jonkin verran kansallisen turvallisuusviranomaisen ja määrättyjen turvallisuusviranomaisten niitä tehtäviä, jotka kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 4 §:n mukaisesti kuuluvat näille viranomaisille.

5 Asian valmistelu

Hallituksen esitys on valmisteltu ulkoasiainministeriössä. Sopimuksen valmisteluun ja neuvotteluihin on osallistunut edustajia ulkoasiainministeriöstä, oikeusministeriöstä, puolustusministeriöstä ja Suojelupoliisista. Esityksestä on pyydetty lausunnot oikeusministeriöltä, puolustusministeriöltä, sisäministeriöltä, valtiovarainministeriöltä, liikenne- ja viestintäministeriöltä, työ- ja elinkeinoministeriöltä, Suojelupoliisilta ja Viestintävirastolta. Lausunnot on saatu puolustusministeriöltä, sisäministeriöltä, liikenne- ja viestintäministeriöltä sekä työ- ja elinkeinoministeriöltä. Lausunnoissa on puollettu sopimuksen hyväksymistä ja voimaansaattamista.

YKSITYISKOHTAISET PERUSTELUT

1 Sopimuksen sisältö ja suhde Suomen lainsäädäntöön

1 artikla. *Sopimuksen tarkoitus ja soveltamisala*. Artiklassa määritellään sopimuksen tarkoitukseksi varmistaa Suomen ja Sveitsin välisessä yhteistyössä vaihdetun tai tuotetun turvallisuusluokitellun tiedon suoja. Sopimuksen johdannossa osapuolten välisinä yhteistyöaloina luetellaan ulko-, puolustus-, turvallisuus-, tiede- ja yritysasiat sekä tekniset asiat.

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

Artiklan a kohdassa on turvallisuusluokitellun tiedon määritelmä. Sopimus koskee missä tahansa muodossa olevaa, minkä tahansa luonteista ja millä tavalla tahansa välitettävää tietoa, asiakirjaa tai aineistoa, jonka osapuoli luovuttaa toiselle osapuolelle ja joka on turvallisuusluokiteltu ja johon on tehty asianmukainen luokitusmerkintä kansallisten säädösten ja määräysten mukaisesti. Sopimus koskee myös tietoa, asiakirjaa tai aineistoa, joka on tuotettu tällaisen turvallisuusluokitellun tiedon pohjalta ja johon on tehty asianmukainen luokitusmerkintä. Kohta on sopusoinnussa kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 2 §:n 1 kohdan kanssa.

Artiklan b kohdan mukaan turvallisuusluokitellulla sopimuksella tarkoitetaan sopimusta tai alihankintasopimusta, mukaan lukien sopimusta edeltävät neuvottelut, joka sisältää tai johon liittyy turvallisuusluokiteltua tietoa. Kohta on sopusoinnussa kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 2 §:n 3 kohdan kanssa.

Artiklan c kohdan mukaisesti luovuttavalla osapuolella tarkoitetaan osapuolta, joka luovuttaa turvallisuusluokiteltua tietoa. Määritelmä kattaa myös tämän osapuolen lainkäyttövaltaan kuuluvat julkis- tai yksityisoikeudelliset oikeushenkilöt ja luonnolliset henkilöt.

Artiklan d kohdan mukaisesti vastaanottavalla osapuolella tarkoitetaan osapuolta, jolle luovuttava osapuoli luovuttaa turvallisuusluokiteltua tietoa. Määritelmä kattaa myös tämän osapuolen lainkäyttövaltaan kuuluvat julkis- tai yksityisoikeudelliset oikeushenkilöt ja luonnolliset henkilöt

Artiklan e kohdan mukaan toimivaltaisella turvallisuusviranomaisella tarkoitetaan kansallista turvallisuusviranomaista, määrättyä turvallisuusviranomaista tai muuta toimivaltaista elintä, joka on kansallisten säädösten ja määräysten mukaisesti valtuutettu vastaamaan sopimuksen täytäntöönpanosta. Suomessa mainittuna viranomaisena toimii kansainvälisistä tietoturvallisuusvelvoitteista annetun lain mukaan ulkoasiainministeriö, jossa tehtävää hoitaa Kansallinen turvallisuusviranomainen. Tämän lisäksi puolustusministeriö, pääesikunta, Suojelupoliisi ja Viestintävirasto toimivat määrättyinä turvallisuusviranomaisina.

Artiklan f kohdassa on määritelty tietoturvaloukkaus teoksi tai laiminlyönniksi, joka on vastoin kansallisia säädöksiä ja määräyksiä ja joka voi johtaa turvallisuusluokitellun tiedon katoamiseen tai vaarantumiseen.

Artiklan g kohdassa on määritelty turvallisuusselvitys, jolla tarkoitetaan kansallisten säädösten ja määräysten mukaiseen tutkintamenettelyyn perustuvaa myönteistä arviota siitä, voidaanko oikeushenkilölle tai luonnolliselle henkilölle sallia pääsy tiettyyn turvallisuusluokkaan kuuluvaan turvallisuusluokiteltuun tietoon ja tämän tiedon käsittely.

3 artikla. *Toimivaltaiset turvallisuusviranomaiset*. Artiklan 1 kohdassa on nimetty kummankin osapuolen kansalliset turvallisuusviranomaiset (National Security Authority, NSA), jotka vastaavat sopimuksen yleisestä täytäntöönpanosta. Suomessa kansallisena turvallisuusviranomaisena toimii kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 4 §:n perusteella ulkoasiainministeriö, jossa tehtävää hoitaa Kansallinen turvallisuusviranomainen (NSA). Sveitsissä kansalliseksi turvallisuusviranomaiseksi on nimetty puolustusministeriö, jonka sisällä tehtävää hoitaa tieto- ja tilaturvallisuudesta vastaava osasto (Directorate for Information Security and Facility Protection, IOS).

Artiklan 2 kohdassa velvoitetaan osapuolet ilmoittamaan toisilleen muut toimivaltaiset turvallisuusviranomaiset (Competent Securi-

ty Authorities, CSA), jotka vastaavat sopimuksen eri osien täytäntöönpanosta. Suomessa määrättyjä turvallisuusviranomaisia (Designated Security Authority, DSA) ovat kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 4 §:n mukaisesti puolustusministeriö, pääesikunta, Suojelupoliisi ja Viestintävirasto.

Artiklan 3 kohdassa velvoitetaan osapuolet ilmoittamaan toisilleen mahdolliset myöhemmät toimivaltaisten turvallisuusviranomaisten muutokset.

4 artikla. *Turvallisuusluokitukset.* Artiklan 1 kohdan mukaan sopimuksen mukaisesti luovutettavaan turvallisuusluokiteltuun tietoon merkitään asianmukainen turvallisuusluokka osapuolten kansallisten säädösten ja määräysten mukaisesti.

Artiklan 2 kohdassa määritellään, miten Suomen ja Sveitsin turvallisuusluokituksen tasot vastaavat toisiaan. Sveitsissä turvallisuusluokka merkitään joko saksaksi, ranskaksi tai italiaksi. Korkein, ankarimpia tietoturvallisuustoimenpiteitä vaativa luokka on "ERITTÄIN SALAINEN/YTTERST HEMLIG". Suomessa tähän luokkaan luetaan kuuluviksi tiedot, joiden luvaton ilmitulo voi aiheuttaa erittäin suurta vahinkoa maanpuolustukselle, turvallisuudelle, kansainvälisille suhteille tai muille yleisille eduille. Sveitsillä ei ole käytössään korkeinta merkintää vastaavaa luokkaa, vaan artiklan 5 kohdassa lähdetään siitä, että jos Suomi lähettäisi Sveitsille luokkaan ERITTÄIN SALAINEN/YTTERST HEMLIG luokiteltua tietoa, toimivaltaiset turvallisuusviranomaiset sopisivat erikseen tiedon käsittelystä. Toiseksi korkein turvallisuusluokka on "SALAINEN/HEMLIG" (GEHEIM/SECRET/ SEGRETO). 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" (VERTRAULICH/CONFIDENTIEL/ CONFIDENZIALE), jolla tarkoitetaan Suomessa tietoja, joiden luvaton ilmitulo voi aiheuttaa vahinkoa maanpuolustukselle, turvallisuudelle, kansainvälisille suhteille tai muille yleisille eduille. Neljänteen asiakirjaluokkaan "KÄYTTÖ RAJOITETTU/BEGRÄNSAD TILLGÅNG" (INTERN/INTERNE/AD USO INTERNO) kuuluvat tiedot, joiden luvaton ilmitulo voi aiheuttaa haittaa yleisille eduille tai heikentää viranomaisen toimintaedellytyksiä.

Suomen kansainvälisiä suhteita suojaavat julkisuuslain 24 §:n 1 momentin 1 ja 2 kohta, maanpuolustusta momentin 10 kohta ja turvallisuutta momentin 5, 8 ja 9 kohta. Muita julkisuuslaissa 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). Julkisuuslain 25 §:ssä on yleiset säännökset salassapito- ja luokitusmerkinnän tekemisestä viranomaisen asiakirjaan. Lain 25 §:n 3 momentin mukaan asiakirjaan voidaan tehdä merkintä sen osoittamiseksi, minkälaisia tietoturvallisuusvaatimuksia asiakirjaa käsiteltäessä noudatetaan. Kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa tarkoitettuihin asiakirjoihin on tehtävä turvallisuusluokituksesta merkintä siten kuin tässä laissa säädetään. Turvallisuusluokituksesta on tehtävä merkintä myös, jos valtioneuvoston antamalla asetuksella niin säädetään.

Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 8 §:n mukaan erityissuojattavaan tietoaineistoon on siitä riippumatta, mitä viranomaisen toiminnan julkisuudesta annetussa laissa tai sen nojalla säädetään, tehtävä kansainvälisessä tietoturvallisuusvelvoitteessa määritelty luokitusmerkintä sen osoittamiseksi, minkälaisia tietoturvallisuusvaatimuksia sen käsittelyssä on noudatettava. Turvallisuusluokitusmerkintää koskevat erityissäännökset sisältyvät tietoturvallisuusasetuksen 11 §:ään, ja merkintöjen vastaavuudesta kansainvälisten tietoturvallisuusvelvoitteiden luokkien kanssa on säädetty asetuksen 12 §:ssä. Asetuksen 11 §:n 1 momentissa säädetään, milloin salassa pidettävään asiakirjaan voidaan tehdä turvallisuusluokitusmerkintä. Asetuksen 11 §:n 3 momentin mukaan turvallisuusluokitusmerkintää ei saa käyttää muissa kuin 1 momentissa tarkoitetuissa tapauksissa, ellei merkinnän tekeminen ole tarpeen kansainvälisten tietoturvallisuusvelvoitteiden toteuttamiseksi tai asiakirja muutoin liity kansainväliseen yhteistyöhön. Ruotsinkielisistä turvallisuus-

luokitusmerkinnöistä on erityissäännös asetuksen 11 §:n 4 momentissa.

Artiklan 3 kohdassa todetaan, että englanninkieliset luokitusta koskevat merkinnät TOP SECRET, SECRET, CONFIDENTIAL ja RESTRICTED vastaavat taulukossa ilmenevällä tavalla Suomen ja Sveitsin turvallisuusluokitusmerkintöjä.

Artiklan 4 kohdan mukaan vastaanottajan tulee varmistaa, ettei turvallisuusluokkaa muuteta eikä kumota ilman luovuttavan osapuolen antamaa kirjallista lupaa.

5 artikla. *Turvallisuusluokitellun tiedon suojaaminen.* Artikla sisältää keskeiset vastavuoroista suojaamista koskevat velvoitteet.

Artiklan 1 kohdassa osapuolet velvoitetaan toteuttamaan kaikki asianmukaiset kansallisten säädöstensä ja määräystensä mukaiset toimenpiteet suojatakseen sopimuksen mukaisesti luovutettua turvallisuusluokiteltua tietoa ja antaakseen sille saman suojan kuin omalle vastaavaan turvallisuusluokkaan kuuluvalle tiedolleen.

Artiklan 2 kohta kieltää luovuttamasta turvallisuusluokiteltuja tietoja kolmannelle osapuolelle ilman luovuttavan osapuolen kirjallista ennakkosuostumusta. Kohta velvoittaa osapuolet noudattamaan luovuttajan suostumuksen periaatetta.

Artiklan 3 kohta koskee henkilöstöturvallisuutta. Sen mukaan turvallisuusluokiteltua tietoa voivat saada vain henkilöt, joilla on tiedonsaantitarve ja joista on tehty kansallisen lainsäädännön mukainen turvallisuusselvitys ja joille on annettu lupa saada kyseistä turvallisuusluokiteltua tietoa. Lisäksi henkilöille tulee olla selvitettynä heidän vastuunsa turvallisuusluokitellun tiedon suojaamisesta. Määräys on sopusoinnussa kansainvälisen tietoturvallisuusvelvoitteista annetun lain 6 §:n 3 momentin kanssa, jossa sallitaan tietoaineistoon pääsy vain niille henkilöille, jotka tarvitsevat tietoja tehtävänsä hoitamiseen. Kansainvälisen tietoturvallisuusvelvoitteen edellyttämä henkilöiden luotettavuuden varmistaminen toteutetaan Suomessa turvallisuusselvityksistä annetun lain sekä kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 11 §:n mukaisesti. Henkilöturvallisuusselvityksen laatii pääesikunta silloin, kun kysymys on puolustushallintoon liittyvästä asiasta, muutoin Suojelupoliisi.

Artiklan 4 kohdan mukaan turvallisuusluokiteltua tietoa saa käyttää ainoastaan siihen tarkoitukseen, jota varten se on annettu. Velvoitetta vastaava säännös on kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 6 §:n 2 momentissa.

6 artikla. *Turvallisuusluokitellut sopimukset.* Artikla sisältää määräykset 2 artiklan b kohdassa tarkoitetun turvallisuusluokitellun sopimuksen tekemisestä jommankumman osapuolen alueella.

Artiklan 1 kohdan mukaan vastaanottavan osapuolen toimivaltainen turvallisuusviranomainen ilmoittaa pyynnöstä luovuttavan osapuolen toimivaltaisen turvallisuusviranomaiselle, onko ehdotetulla hankeosapuolella vaadittavaa turvallisuusluokkaa vastaava todistus yhteisöturvallisuusselvityksestä (Facility Security Clearance, FSC). Jos kyseessä olevalla hankeosapuolella ei ole vaadittavaa todistusta yhteisöturvallisuusselvityksestä, luovuttavan osapuolen toimivaltainen turvallisuusviranomainen voi pyytää, että vastaanottajan toimivaltainen turvallisuusviranomainen tekisi hankeosapuolta koskevan turvallisuusselvityksen.

Artiklan 2 kohdan mukaan avoimessa tarjouskilpailutilanteessa vastaanottajan toimivaltainen turvallisuusviranomainen voi ilman virallista pyyntöä toimittaa luovuttavan osapuolen toimivaltaiselle turvallisuusviranomaiselle asiaankuuluvat todistukset turvallisuusselvityksestä.

Artiklan 3 kohta asettaa velvoitteen sisällyttää turvallisuusluokiteltuihin sopimuksiin asianmukaiset turvallisuusmääräykset, mukaan lukien luokitusohjeet. Kopio turvallisuusmääräyksistä toimitetaan sen osapuolen toimivaltaiselle turvallisuusviranomaiselle, jonka lainkäyttövallan alaisuudessa sopimus toteutetaan. Turvallisuusluokiteltuja sopimuksia koskevat kansalliset säännökset sisältyvät kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 1 § 2 momenttiin (soveltaminen elinkeinonharjoittajaan), 2 §:n 2 kohtaan (erityissuojattava tietoaineisto), 7 §:ään (vaitiolovelvollisuus ja hyväksikäyttökielto) sekä 12 §:ään (yhteisöturvallisuusselvitys), 13 §:ään (sitoumus turvallisuustoimenpiteiden suorittamisesta) ja 14 §:ään (turvallisuustodistus). Kansallinen sääntely vastaa sopimusvelvoitteen vaatimuksia. Velvoitteen täyttämiseksi tarpeellisesta suoma-

laisen viranomaisen tietojenanto-oikeudesta säädetään kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 17 §:ssä.

Artiklan 4 kohdan mukaan osapuolten toimivaltaisten turvallisuusviranomaisten edustajat voivat vierailla toistensa luona analysoidakseen hankeosapuolen turvallisuusluokitellun tiedon suojaamiseksi toteuttamien toimenpiteiden tehokkuutta. Määräyksellä on yhteys myös turvallisuusyhteistyötä koskevaan sopimuksen 10 artiklan 2 kohtaan, jossa määrätään osapuolten turvallisuusviranomaisten vierailuista.

7 artikla. *Turvallisuusluokitellun tiedon välittäminen ja rekisteröinti.* Artikla sisältää määräykset menettelyistä siirrettäessä turvallisuusluokiteltuja tietoja osapuolten kesken.

Tieto välitetään 1 kohdan mukaan osapuolten kansallisten säädösten ja määräysten mukaisesti hallitukselta hallitukselle suojattuja kanavia käyttäen tai muita toimivaltaisen turvallisuusviranomaisten keskenään sopimia keinoja käyttäen. Määräys on sopusoinnussa tietoturvallisuusasetuksen asiakirjan välittämistä koskevan 18 §:n ja asiakirjan siirtämistä tietoverkossa koskevan19 §:n kanssa. Artiklan 2 kohdan mukaan turvallisuusluokkaan LUOTTAMUKSELLINEN/ KONFIDENTIELL tai sitä korkeampaan luokkaan luokiteltu tieto on vaihdettava ja rekisteröitävä kansallisen lainsäädännön edellyttämällä tavalla. Määräys on sopusoinnussa tietoturvallisuusasetuksen käsittelyn kirjaamista koskevan 20 §:n kanssa, jonka mukaan suojaustasoon I-III kuuluvien asiakirjojen käsittely tulee kirjata sähköiseen lokiin, tietojärjestelmään, asianhallintajärjestelmään, manuaaliseen diaariin tai asiakirjaan.

8 artikla. *Turvallisuusluokitellun tiedon kääntäminen, kopiointi ja hävittäminen.* Artikla sisältää määräykset siitä, miten eri turvallisuusluokkiin kuuluvia aineistoja saa kääntää, kopioida ja hävittää.

Artiklan 1 kohdassa velvoitetaan tekemään turvallisuusluokitellun tiedon käännöksiin ja kopioihin samat turvallisuusluokitusmerkinnät kuin alkuperäiseen ja suojaamaan niitä merkintöjen mukaisesti. Kopioita otetaan ainoastaan viralliseen tarkoitukseen tarvittava vähimmäismäärä.

Artiklan 2 kohdassa velvoitetaan tekemään käännöksiin asianmukainen käännöskielinen merkintä siitä, että käännökset sisältävät turvallisuusluokiteltua tietoa.

Artiklan 3 kohdan mukaan turvallisuusluokkaan SALAINEN/HEMLIG tai sitä korkeampaan luokkaan kuuluvaa tietoa saa kääntää tai kopioida ainoastaan luovuttajan kirjallisella suostumuksella.

Artiklan 4 kohdan mukaan turvallisuusluokkaan SALAINEN/HEMLIG kuuluvaa tietoa ei saa hävittää ilman luovuttavan osapuolen kirjallista ennakkosuostumusta. Se palautetaan luovuttavalle osapuolelle sen jälkeen, kun osapuolet katsovat, ettei tietoa enää tarvita.

Artiklan 5 kohdan mukaan turvallisuusluokkaan LUOTTAMUKSELLINEN/ KONFIDENTIELL kuuluva tieto hävitetään sen jälkeen, kun sitä ei enää katsota tarvittavan.

Artiklan 6 kohta sisältää määräyksen kriisitilanteen varalle. Kohdassa velvoitetaan hävittämään sopimuksen perusteella luovutettu turvallisuusluokiteltu tieto välittömästi, jos kriisitilanne estää tiedon suojaamisen. Hävittämisestä tulee ilmoittaa mahdollisimman pian luovuttavan osapuolen toimivaltaiselle turvallisuusviranomaiselle.

Velvollisuudesta pitää huolta erityissuojattavan tietoaineiston suojaamisesta sen turvallisuusluokkaa vastaavalla tavalla sitä luotaessa, kopioitaessa, siirrettäessä, jaettaessa, säilytettäessä, hävitettäessä tai muutoin käsiteltäessä on säädetty kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 9 §:n 1 momentissa. Tarkemmat käsittelyä koskevat määräykset on Suomessa säädetty asetuksentasoisina Julkisuuslain nojalla säädetyn tietoturvallisuusasetuksen 17 §:ssä säädetään asiakirjan kopioimisesta ja 21 §:ssä asiakirjan arkistoimisesta ja hävittämisestä..

9 artikla. *Vierailut.* Artiklaa sovelletaan vierailuihin, joihin liittyy mahdollisuus saada turvallisuusluokiteltua tietoa. Artiklan 1 kohdan mukaan tällaiseen vierailuun vaaditaan isäntäosapuolen toimivaltaisen turvallisuusviranomaisen ennakolta antama kirjallinen lupa. Vierailijoiden sallitaan saada turvallisuusluokiteltua tietoa ainoastaan, jos heillä on lähettävän osapuolen toimivaltaisen turvallisuusviranomaisen lupa vierailuun tai vierailuihin (a alakohta), heille on annettu asianmukainen todistus henkilöturvallisuusselvityksestä (b alakohta) ja heillä on lupa ottaa vastaan turvallisuusluokiteltua tietoa isän-

täosapuolen kansallisten säädösten ja määräysten mukaisesti (c alakohta).

Artiklan 2 kohta sisältää määräykset niistä menettelytavoista, joita noudatetaan järjestettäessä vierailuja. Kohdassa asetetun määräajan mukaan isäntäosapuolen toimivaltaisen turvallisuusviranomaisen tulee saada vierailupyyntö 14 päivää ennen vierailun aiottua ajankohtaa. Kiireellisissä tapauksissa toimivaltaiset turvallisuusviranomaiset voivat sopia lyhyemmästä ajankohdasta. Vierailupyynnön on sisällettävä sopimuksen liitteessä 2 edellytetyt tarkemmat tiedot vierailijasta ja vierailusta.

Artiklan 3 kohdan mukaan vierailuluvan enimmäisvoimassaoloaika on korkeintaan 12 kuukautta.

10 Artikla. *Turvallisuusyhteistyö.* Artiklan 1 kohdassa kansalliset turvallisuusviranomaiset velvoitetaan antamaan toisilleen tiedoksi turvallisuusluokitellun tiedon suojaamista koskevat kansalliset säädöksensä ja määräyksensä sekä niiden mahdolliset muutokset.

Artiklan 2 kohdan mukaan läheisen yhteistyön varmistamiseksi sopimuksen täytäntöönpanossa toimivaltaiset turvallisuusviranomaiset neuvottelevat tarvittaessa keskenään ja antavat pyynnöstä toisilleen tietoa turvallisuusluokitellun tiedon suojaamista koskevista kansallisista turvallisuusnormeistaan, menettelyistään ja käytännöistään. Tätä tarkoitusta varten toimivaltaiset turvallisuusviranomaiset voivat tehdä keskinäisiä vierailuja. Vierailujen toteuttamiseen liittyvät säännökset ovat kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 18 §:ssä.

Artiklan 3 kohdan mukaan toimivaltaiset turvallisuusviranomaiset avustavat pyynnöstä toisiaan osapuolten kansallisten säädösten ja määräysten mukaisesti yhteisö- ja henkilöturvallisuusselvitysten tekemisessä.

Artiklan 4 kohdan mukaan kansalliset turvallisuusviranomaiset ilmoittavat viipymättä toisilleen muutoksista asianomaisiin turvallisuustodistuksiin.

Artiklan 5 kohdassa todetaan, että sopimusta ei sovelleta turvallisuusluokitellun tiedon vaihtoon, jota vaihdetaan osapuolten tiedustelupalveluiden tai lainvalvontaviranomaisten, kuten poliisin, välillä.

11 artikla. *Tietoturvaloukkaukset.* Artiklan 1 kohdassa osapuolet velvoitetaan ilmoittamaan viipymättä toisilleen epäillystä tai todetusta tietoturvaloukkauksesta.

Artiklan 2 kohdan mukaan osapuolet sitoutuvat tutkimaan tapaukset viipymättä kansainvälisen oikeuden ja kansallisen lainsäädännön asettamissa rajoissa. Toinen osapuoli tekee tarvittaessa tutkintayhteistyötä toimivaltaisen osapuolen kanssa. Artiklan 3 kohdan mukaan osapuolet ryhtyvät kaikkiin tarpeellisiin toimenpiteisiin kansainvälisen oikeuden ja kansallisen lainsäädännön asettamissa rajoissa rajoittaakseen tietoturvaloukkauksen seurauksia ja estääkseen uusia loukkauksia. Toiselle osapuolelle on ilmoitettava tutkinnan ja toteutettujen toimien tuloksista. Artiklan velvoitteisiin liittyvät säännökset sisältyvät kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 19 §:ään.

12 artikla. *Kustannukset.* Artiklan mukaan kumpikin osapuoli vastaa omista sopimuksesta johtuvien velvoitteiden täyttämisestä aiheutuvista kustannuksistaan.

13 artikla. *Riitojen ratkaiseminen.* Artiklan mukaan kaikki sopimuksen tulkintaan tai soveltamiseen liittyvät osapuolten väliset riidat ratkaistaisiin yksinomaan osapuolten välisissä neuvotteluissa.

14 artikla. *Loppumääräykset.* Artiklassa on sopimuksen voimaantuloa, muuttamista ja irtisanomista koskevat määräykset sekä irtisanomisesta johtuvat velvollisuudet. Sopimus on voimassa toistaiseksi. Sopimusta voidaan muuttaa osapuolten keskinäisellä kirjallisella suostumuksella. Osapuoli voi irtisanoa sopimuksen ilmoittamalla asiasta kirjallisesti toiselle osapuolelle diplomaattiteitse kuuden kuukauden irtisanomisaikaa noudattaen.

Sopimuksen lopussa on todettu, että sopimus korvaa voimaantullessaan puolustusministeriöiden välillä Bernissä 17 päivänä maaliskuuta 1994 allekirjoitetun yhteisymmärryspöytäkirjan turvallisuusluokitellun tiedon vaihtamisesta.

2 Lakiehdotuksen perustelut

Suomen perustuslain 95 §:ssä edellytetään, että kansainvälisen velvoitteen lainsäädännön alaan kuuluvat määräykset saatetaan valtionsisäisesti voimaan erityisellä voimaansaattamislailla. Tällaiset määräykset tulee saattaa voimaan lailla myös silloin, kun velvoitteen

johdosta ei ole tarpeen tarkistaa kansallisen lainsäädännön aineellista sisältöä. Koska Suomen ja Sveitsin välisen tietoturvallisuussopimuksen 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 §. Sopimuksen muiden kuin lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta ja lain voimaantulosta säädettäisiin valtioneuvoston asetuksella. Laki on tarkoitus saattaa voimaan samanaikaisesti kuin sopimus tulee Suomen osalta voimaan.

3 Voimaantulo

Suomen ja Sveitsin välisen sopimuksen 14 artiklan 1 kohdan mukaan osapuolet ilmoittavat toisilleen, kun sopimuksen voimaantulon edellyttämät kansalliset toimenpiteet on toteutettu. Sopimus tulee voimaan toiseksi seuraavan kuukauden ensimmäisenä päivänä sen jälkeen, kun jälkimmäinen ilmoitus on otettu vastaan.

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

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 tarkoittamasta asiasta on perustuslain mukaan säädettävä lailla tai jos määräyksessä tarkoitetusta asiasta on jo voimassa lain säännöksiä taikka siitä on Suomessa vallitsevan käsityksen mukaan säädettävä lailla. Perustuslakivaliokunnan 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 2 artiklassa määritellään, mitä tarkoitetaan turvallisuusluokitellulla tiedolla, turvallisuusluokitelluilla sopimuksilla, turvallisuusselvityksillä ja tietoturvaloukkauksella. Koska nämä määritelmät vaikuttavat joko suoraan tai välillisesti sopimuksen lainsäädännön alaan kuuluvien aineellisten määräysten tulkintaan ja soveltamiseen, ne edellyttävät eduskunnan hyväksymistä (PeVL 6/2001 vp).

Sopimuksen 3 artiklassa määritellään Suomen kansalliseksi turvallisuusviranomaiseksi ulkoasiainministeriö. Sopimusmääräys vastaa kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 4 §:n 1 momenttia. Määräys on siten toteava, eikä sen siten ole katsottava edellyttävän eduskunnan hyväksymistä.

Sopimuksen 4 artiklassa on määräykset turvallisuusluokitusmerkinnän tekemisestä ja turvallisuusluokkien vastaavuudesta. Yleisesti sovellettavat säännökset salassapito- ja luokitusmerkinnästä on säädetty julkisuuslain 25 §:ssä. Sen mukaan salassa pidettävään viranomaisen asiakirjaan on tehtävä merkintä asiakirjan salassa pitämisestä, kun tällainen asiakirja annetaan asianosaiselle ja kun asiakirja on pidettävä salassa toisen tai yleisen edun vuoksi. Muihin salaisiin asiakirjoihin tehtävä merkintä on harkinnanvarainen. Lisäksi kansainvälisistä tietoturvavelvoitteista annetun lain 8 §:ssä on säännökset turvallisuusluokan merkitsemisestä erityissuojattavaan tietoaineistoon. Sen mukaisesti erityissuojattavaan tietoaineistoon on julkisuuslain säännöksistä riippumatta tehtävä kansainvälisessä tietoturvallisuusvelvoitteessa määritelty merkintä sen osoittamiseksi, millaisia tieto-

turvallisuusvaatimuksia käsittelyssä on noudatettava. Määräys kuuluu lainsäädännön alaan.

Sopimuksen 5 artiklassa määrätään sopimuksen soveltamisalan piiriin kuuluvan turvallisuusluokitellun tiedon suojaamiseksi tarvittavista toimenpiteistä, jotka rajoittavat turvallisuusluokitellun tiedon luovuttamista sekä sen välittämistä, käyttämistä ja pääsyä siihen. Sopimuksen 5 artiklassa on kyse sopimuksen ydinmääräyksestä, jonka perusteella Suomi voi suojata sopimuksen perusteella vaihdettua turvallisuusluokiteltua tietoa ilman julkisuuslaissa säädettyä vahinkoedellytysarviointia. 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. Julkisuuslain säännöksistä poiketen kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 6 §:n 1 momentin mukaan erityissuojattava tietoaineisto on pidettävä salassa, jollei kansainvälisistä tietoturvallisuusvelvoitteesta muuta johdu. Sopimuksen 5 artiklan 3 kohdassa on ilmaistu myös turvallisuusluokiteltua tietoa saavia henkilöitä koskeva rajoitus. Artiklan 3 kohdassa määrätään osapuolten velvollisuudesta teettää asianmukainen turvallisuusselvitys henkilöistä, joilla on tai saattaa olla pääsy sopimuksessa tarkoitettuun turvallisuusluokiteltuun tietoon. Turvallisuusselvitysten laadinnassa on otettava huomioon perustuslain 10 §:n 1 momentissa säädetty yksityiselämän suoja ja velvollisuus säätää henkilötietojen suojasta lailla. Suomessa turvallisuusselvityksen kohteena olevista henkilöistä sekä selvityksessä sovellettavasta menettelystä on säädetty turvallisuusselvityksistä annetussa laissa. Määräys kuuluu siten lainsäädännön alaan ja edellyttää eduskunnan suostumusta voimaantullakseen. Sopimuksen 5 artiklan 4 kohdan mukaan turvallisuusluokiteltua tietoa saa käyttää ainoastaan siihen tarkoitukseen, jota varten se on annettu. Velvoitetta vastaava säännös on kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 6 §:n 2 momentissa. Kohdan määräys kuuluu näin ollen lainsäädännön alaan.

Sopimuksen 6 artiklassa on määräykset turvallisuusluokitelluista sopimuksista ja niitä tekevien yritysten turvallisuusselvityksistä. Yhteisöturvallisuusselvitystä koskevat säännökset sisältyvät kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 12 ja 13 §:ään. Osapuolten turvallisuusviranomaisten vierailuihin liittyy sopimuksen 6 artiklan 4 kohta, jossa mahdollistetaan osapuolten toimivaltaisten turvallisuusviranomaisten vierailu toistensa luona. Osapuolten edustajien vierailuiden tarkoituksena on varmistaa sopimuksen tarkoituksen toteuttaminen turvallisuusluokiteltujen tietojen asianmukaiseksi suojaamiseksi. Tähän vierailuoikeuteen ei sisälly sellaista julkista vallan käyttöä ja tarkastusoikeutta, joka olisi ristiriidassa perustuslain kanssa (PeVL 39/1997). Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 18 §:ssä on vastaavat säännökset vierailuja koskevan sopimusmääräyksen täytäntöönpanoon liittyvistä seikoista. Artikla kuuluu lainsäädännön alaan lukuun ottamatta 2 kohtaa, jota ei ole kirjoitettu velvoittavaan muotoon.

Sopimuksen 11 artiklassa edellytetään, että kumpikin osapuoli ilmoittaa viipymättä toiselle osapuolelle todetusta tai epäillystä tietoturvaloukkauksesta, joka kohdistuu sopimuksen mukaisesti vaihdettuun turvallisuusluokiteltuun tietoon. Osapuolten on lisäksi toteutettava kansallisten lakiensa ja määräystensä mukaisesti kaikki asianmukaiset toimenpiteet rajoittaakseen tietoturvaloukkauksen seurauksia ja tutkittava tapaus. Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 19 §:ssä säädetään kansalliselle turvallisuusviranomaiselle kuuluvista velvoitteista sopimusmääräyksissä tarkoitetuissa tilanteissa. Artiklan määräykset kuuluvat näin ollen lainsäädännön alaan.

4.2 Käsittelyjärjestys

Turvallisuusluokitellun tietoaineiston salassapidosta on annettu yleiset säännökset laissa kansainvälisistä tietoturvallisuusvelvoitteista. Sen 6 §:n 1 momentin mukaan erityissuojattava tietoaineisto on pidettävä salassa, jollei kansainvälisestä tietoturvallisuusvelvoitteesta muuta johdu. Lain 6 §:n 2 momentin mukaan 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. Edelleen lain 6 §:n 3 momentin mukaan erityissuojattavaa tietoaineistoa käsittelevän viranomaisen on pidettävä huolta siitä, että tietoaineistoon on pääsy vain niillä, jotka tarvitsevat tietoja tehtävänsä hoitamisessa. Nämä henkilöt on nimettävä etukäteen kansainvälisessä tietoturvallisuusvelvoitteessa edellytetyissä tapauksissa. Sama koskee myös 1 §:n 2 momentissa tarkoitettua elinkeinonharjoittajaa. Erityissuojattavalla tietoaineistolla tarkoitetaan laissa sellaisia salassa pidettäviä asiakirjoja ja materiaaleja sekä asiakirjoista ja materiaaleista saatavissa olevia tietoja sekä näiden perusteella tuotettuja asiakirjoja ja materiaaleja, jotka kansainvälisen tietoturvallisuusvelvoitteen mukaisesti on turvallisuusluokiteltu. Käsillä olevan sopimuksen 5 artiklan määräykset eivät laajenna salassapitovelvollisuutta siitä, mitä salassapidosta on säädetty sanotun lain 6 §:ssä. Määräykset eivät siten vaikuta sopimuksen käsittelyjärjestykseen.

Suomen ja Sveitsin välillä turvallisuusluokitellun tiedon vastavuoroisesta suojaamisesta tehtyyn sopimukseen ei voida katsoa sisältyvän sellaisia määräyksiä, jotka koskisivat perustuslakia sen 94 §:n 2 momentissa ja 95 §:n 2 momentissa tarkoitetulla tavalla. Hallituksen näkemyksen mukaan sopimus voitaisiin näin ollen hyväksyä äänten enemmistöllä ja ehdotus sen lainsäädännön alaan kuuluvien sopimusmääräysten voimaansaattamiseksi tavallisen lain säätämisjärjestyksessä.

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

> *eduskunta hyväksyisi turvallisuusluokitellun tiedon vastavuoroisesta suojaamisesta Suomen tasavallan hallituksen ja Sveitsin liittoneuvoston hallituksen välillä Solothurnissa 28 päivänä tammikuuta 2014 tehdyn sopimuksen.*

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

Lakiehdotus

Laki

turvallisuusluokitellun tiedon vastavuoroisesta suojaamisesta Sveitsin kanssa tehdyn sopimuksen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta

Eduskunnan päätöksen mukaisesti säädetään:

1 §

Turvallisuusluokitellun tiedon vastavuoroisesta suojaamisesta Suomen tasavallan hallituksen ja Sveitsin liittoneuvoston välillä Solothurnissa 28 päivänä tammikuuta 2014 tehdyn sopimuksen lainsäädännön alaan kuuluvat määräykset ovat lakina voimassa sellaisina kuin Suomi on niihin sitoutunut.

2 §

Sopimuksen muiden määräysten voimaansaattamisesta ja tämän lain voimaantulosta säädetään valtioneuvoston asetuksella.

Helsingissä 28 päivänä toukokuuta 2014

Pääministeri

JYRKI KATAINEN

Ulkoasiainministeri *Erkki Tuomioja*

Suomennos

SOPIMUS SUOMEN TASAVALLAN HALLITUKSEN JA SVEITSIN LIITTONEUVOSTON VÄLILLÄ TURVALLISUUSLUOKITELLUN TIEDON VASTAVUOROISESTA SUOJAAMISESTA

Suomen tasavallan hallitus ja Sveitsin liittoneuvosto, jäljempänä "osapuolet", jotka

pitävät mielessä, että osapuolet voivat vaihtaa mutta eivät ole velvollisia vaihtamaan keskenään turvallisuusluokiteltua tietoa tämän sopimuksen mukaisesti,

tiedostavat, että turvallisuusluokiteltua tietoa vaihdettaessa sitä on käsiteltävä tällä sopimuksella määrättyjä periaatteita noudattaen,

suojatakseen turvallisuusluokiteltua tietoa, joka liittyy esimerkiksi ulko-, puolustus-, turvallisuus-, tiede- tai yritysasioihin tai teknisiin asioihin ja jota vaihdetaan suoraan osapuolten välillä tai niiden lainkäyttövaltaan kuuluvien turvallisuusluokiteltua tietoa käsittelevien julkis- tai yksityisoikeudellisten oikeushenkilöiden tai luonnollisten henkilöiden välillä,

ovat sopineet seuraavasta:

1 artikla

Tarkoitus ja soveltamisala

Tämän sopimuksen tarkoituksena on varmistaa sellaisen turvallisuusluokitellun tiedon suojaaminen, jota vaihdetaan tai tuotetaan osapuolten välisessä yhteistyössä.

2 artikla

Määritelmät

Tässä sopimuksessa

a) *turvallisuusluokiteltu tieto* tarkoittaa missä tahansa muodossa olevaa, minkä tahansa luonteista ja millä tavalla tahansa välitettävää tietoa, asiakirjaa tai aineistoa, jonka osapuoli luovuttaa toiselle osapuolelle ja joka on tur-

Sopimusteksti

AGREEMENT BETWEEN THE GOVERNMENT OF THE REPUBLIC OF FINLAND AND THE SWISS FEDERAL COUNCIL ON MUTUAL PROTECTION OF CLASSIFIED INFORMATION

The Government of the Republic of Finland and the Swiss Federal Council, hereinafter referred to as "the Parties",

bearing in mind that the Parties may but are not obliged to exchange Classified Information in the framework of this Agreement

recognising that when exchanging Classified Information it shall be handled in accordance with the principles governed in this Agreement

in order to protect Classified Information relating for example to foreign affairs, defence, security or scientific, industrial and technological matters and exchanged directly between the Parties, or public or private legal entities or individuals that deal with Classified Information under the jurisdiction of the Parties,

have agreed as follows:

Article 1

Purpose and scope of application

The purpose of this Agreement is to ensure the protection of Classified Information that is exchanged or created in the process of cooperation between the Parties.

Article 2

Definitions

For the purposes of this Agreement:

a) *Classified Information* means any information, document or material of whatever form, nature or method of transmission provided by one Party to the other Party and to which a security classification level has been

vallisuusluokiteltu ja johon on tehty asianmukainen luokitusmerkintä kansallisten säädösten ja määräysten mukaisesti, sekä tietoa, asiakirjaa tai aineistoa, joka on tuotettu tällaisen turvallisuusluokitellun tiedon pohjalta ja johon on tehty asianmukainen luokitusmerkintä;

b) *turvallisuusluokiteltu sopimus* tarkoittaa sopimusta tai alihankintasopimusta, mukaan lukien sopimusta edeltävät neuvottelut, joka sisältää tai johon liittyy turvallisuusluokiteltua tietoa;

c) *luovuttava osapuoli* tarkoittaa sitä osapuolta sekä sen lainkäyttövaltaan kuuluvaa julkis- tai yksityisoikeudellista oikeushenkilöä tai luonnollista henkilöä, joka luovuttaa turvallisuusluokiteltua tietoa;

d) *vastaanottava osapuoli* tarkoittaa sitä osapuolta sekä sen lainkäyttövaltaan kuuluvaa julkis- tai yksityisoikeudellista oikeushenkilöä tai luonnollista henkilöä, jolle luovuttava osapuoli luovuttaa turvallisuusluokiteltua tietoa.

e) *toimivaltainen turvallisuusviranomainen* tarkoittaa kansallista turvallisuusviranomaista, määrättyä turvallisuusviranomaista tai muuta toimivaltaista elintä, joka on osapuolten kansallisten säädösten ja määräysten mukaisesti valtuutettu vastaamaan tämän sopimuksen täytäntöönpanosta;

f) *tietoturvaloukkaus* tarkoittaa kansallisten säädösten ja määräysten vastaista tekoa tai laiminlyöntiä, jonka johdosta turvallisuusluokiteltu tieto saattaa kadota tai vaarantua;

g) *turvallisuusselvitys* tarkoittaa kansallisten säädösten ja määräysten mukaiseen tutkintamenettelyyn perustuvaa myönteistä arviota siitä, voidaanko oikeushenkilölle (yhteisöturvallisuusselvitys) tai luonnolliselle henkilölle (henkilöturvallisuusselvitys) sallia pääsy tiettyyn turvallisuusluokkaan kuuluvaan turvallisuusluokiteltuun tietoon ja tämän tiedon käsittely.

applied and which has been marked accordingly under national laws and regulations, as well as any information, document or material that has been generated on the basis of such Classified Information and marked accordingly;

b) *Classified Contract* means any contract or sub-contract, including pre-contractual negotiations, which contains or involves Classified Information;

c) *Originating* Party means the Party, as well as any public or private legal entity or individual under its jurisdiction, releasing Classified Information;

d) *Receiving Party* means the Party, as well as any public or private legal entity or individual under its jurisdiction, to which the Classified Information is released by the Originating Party;

e) *Competent Security Authority* means a National Security Authority, a Designated Security Authority or any other competent body authorised according to the national laws and regulations of the Parties which is responsible for the implementation of this Agreement;

f) *Breach of Security* means an act or an omission contrary to national laws and regulations which may lead to the loss or compromise of Classified Information;

g) *Security Clearance* means a positive determination following an investigative procedure in accordance with national laws and regulations to ascertain the eligibility of an entity (Facility Security Clearance, FSC) or individual (Personnel Security Clearance, PSC) to have access to and to handle Classified Information on a certain level.

3 artikla

Toimivaltaiset turvallisuusviranomaiset

1. Osapuolet ovat nimenneet seuraavat kansalliset turvallisuusviranomaiset (National Security Authority, NSA) vastaamaan yleisesti tämän sopimuksen täytäntöönpanosta:

Article 3

Competent Security Authorities

1. The National Security Authorities (NSAs) designated by the Parties as responsible for the general implementation of this Agreement are:

Suomen tasavalta	Sveitsin valaliitto
Ulkoasiainministeriö *Kansallinen* *turvallisuusviranomainen* *(NSA)* *SUOMI*	*Ministry of Defence* *Directorate for* *Information Security and* *Facility Protection (IOS)* *SWITZERLAND*

In the Republic of Finland	In the Swiss Confederation
Ministry for Foreign Affairs *National Security* *Authority* *(NSA)* *FINLAND*	*Ministry of Defence* *Directorate for* *Information Security and* *Facility Protection (IOS)* *SWITZERLAND*

2. Osapuolet antavat toisilleen tiedoksi mahdolliset muut toimivaltaiset turvallisuusviranomaiset, jotka vastaavat tämän sopimuksen täytäntöönpanosta eri osin.

3. Osapuolet antavat toisilleen tiedoksi mahdolliset myöhemmät toimivaltaisten turvallisuusviranomaisten muutokset.

2. The Parties shall notify each other of any other Competent Security Authorities which shall be responsible for the implementation of aspects of this Agreement.

3. The Parties shall notify each other of any subsequent changes of the Competent Security Authorities.

4 artikla

Turvallisuusluokitukset

1. Tämän sopimuksen mukaisesti luovutettavaan turvallisuusluokiteltuun tietoon merkitään asianmukainen turvallisuusluokka osapuolten kansallisten säädösten ja määräysten mukaisesti.

2. Turvallisuusluokat vastaavat toisiaan seuraavasti:

Article 4

Security classifications

1. Any Classified Information provided under this Agreement shall be marked with the appropriate security classification level under the national laws and regulations of the Parties.

2. The classification levels shall correspond to one another as follows:

Suomen tasavallassa	Sveitsin valaliitossa	Englanninkielinen vastine
ERITTÄIN SALAINEN tai YTTERST HEMLIG	ei vastinetta	TOP SECRET
SALAINEN tai HEMLIG	GEHEIM / SECRET / SEGRETO	SECRET
LUOTTAMUKSELLINEN tai KONFIDENTIELL	VERTRAULICH / CONFIDENTIEL/ CONFIDENZIALE	CONFIDENTIAL
KÄYTTÖ RAJOITETTU tai BEGRÄNSAD TILLGÅNG	INTERN / INTERNE / AD USO INTERNO	RESTRICTED

In the Republic of Finland	In the Swiss Confederation	Equivalent in English
ERITTÄIN SALAINEN or YTTERST HEMLIG	no equivalent	TOP SECRET
SALAINEN or HEMLIG	GEHEIM / SECRET / SEGRETO	SECRET
LUOTTAMUKSELLINEN or KONFIDENTIELL	VERTRAULICH / CONFIDENTIEL/ CONFIDENZIALE	CONFIDENTIAL
KÄYTTÖ RAJOITETTU or BEGRÄNSAD TILLGÅNG	INTERN / INTERNE / AD USO INTERNO	RESTRICTED

3. Tässä sopimuksessa käytettävät englanninkieliset ilmaukset TOP SECRET, SECRET, CONFIDENTIAL ja RESTRICTED vastaavat edellä olevan taulukon suomalaisia ja sveitsiläisiä termejä.

4. Vastaanottava osapuoli varmistaa, ettei turvallisuusluokituksia muuteta eikä kumota ilman luovuttavan osapuolen antamaa kirjallista lupaa.

5. Jos Suomi lähettää turvallisuusluokkaan ERITTÄIN SALAINEN merkittyä turvallisuusluokiteltua tietoa, osapuolten toimivaltaiset turvallisuusviranomaiset sopivat keskenään täydentävistä järjestelyistä.

3. The English expressions TOP SECRET, SECRET, CONFIDENTIAL and RESTRICTED used in this Agreement correspond to the Swiss and Finnish terms in the table above.

4. The Receiving Party shall ensure that classifications are not altered or revoked, except as authorised in writing by the Originating Party.

5. In case Finland sends classified information marked TOP SECRET supplementary arrangements shall be agreed between the respective Competent Security Authorities.

5 artikla

Turvallisuusluokitellun tiedon suojaaminen

1. Osapuolet toteuttavat kaikki asianmukaiset kansallisten säädöstensä ja määräystensä mukaiset toimet suojatakseen tässä sopimuksessa tarkoitettua turvallisuusluokiteltua tietoa. Ne antavat tälle tiedolle samantasoisen suojan kuin omalle vastaavaan turvallisuusluokkaan kuuluvalle tiedolleen.

2. Osapuolet eivät salli kolmansille osapuolille pääsyä turvallisuusluokiteltuun tietoon ilman luovuttavan osapuolen kirjallista ennakkosuostumusta.

3. Pääsy turvallisuusluokiteltuun tietoon sallitaan ainoastaan henkilöille, joilla on tie-

Article 5

Protection of Classified Information

1. The Parties shall take all appropriate measures under their national laws and regulations so as to protect Classified Information referred to in this Agreement. They shall afford such information the same protection as they afford to their own information at the corresponding classification level.

2. The Parties shall not provide access to Classified Information to Third Parties without the prior written consent of the Originating Party.

3. Access to Classified Information shall be limited to individuals who have a 'Need-to-

donsaantitarve, joista on tehty turvallisuusselvitys kansallisten säädösten ja määräysten mukaisesti ja joille on sallittu pääsy tällaiseen tietoon sekä selvitetty heidän vastuunsa turvallisuusluokitellun tiedon suojaamisesta.

4. Turvallisuusluokiteltua tietoa saa käyttää ainoastaan siihen tarkoitukseen, jota varten se on luovutettu.

Know' and who, in accordance with national laws and regulations, have been security cleared and authorised to have access to such information as well as briefed on their responsibilities for the protection of Classified Information.

4. Classified Information shall be used solely for the purpose for which it has been provided.

6 artikla

Turvallisuusluokitellut sopimukset

1. Vastaanottavan osapuolen toimivaltainen turvallisuusviranomainen ilmoittaa pyynnöstä luovuttavan osapuolen toimivaltaiselle turvallisuusviranomaiselle, onko ehdotetulle vastaanottavan osapuolen hankeosapuolelle annettu vaadittua turvallisuusluokkaa vastaava kansallinen todistus turvallisuusselvityksestä. Jollei hankeosapuolella ole todistusta turvallisuusselvityksestä, luovuttavan osapuolen toimivaltainen turvallisuusviranomainen voi pyytää vastaanottavan osapuolen toimivaltaista turvallisuusviranomaista tekemään hankeosapuolta koskevan turvallisuusselvityksen.

2. Jos on kyse avoimesta tarjouskilpailusta, vastaanottavan osapuolen toimivaltaisen turvallisuusviranomaisen olisi annettava luovuttavan osapuolen toimivaltaiselle turvallisuusviranomaiselle asianmukaiset todistukset turvallisuusselvityksestä ilman virallista pyyntöä.

3. Jotta turvallisuutta voitaisiin valvoa ja ohjata riittävästi, tämän sopimuksen liitteessä 1 tarkoitetussa turvallisuusluokitellussa sopimuksessa on oltava asianmukaiset turvallisuusmääräykset, mukaan lukien luokitusohjeet. Kopio turvallisuusmääräyksistä toimitetaan sen osapuolen toimivaltaiselle turvallisuusviranomaiselle, jonka lainkäyttöalueella turvallisuusluokiteltu sopimus pannaan täytäntöön.

4. Osapuolten toimivaltaisten turvallisuusviranomaisten edustajat voivat pyynnöstä vierailla toistensa luona arvioimassa niiden toimien tehokkuutta, jotka hankeosapuoli on toteuttanut suojatakseen turvallisuusluokiteltuun sopimukseen liittyvää turvallisuusluokiteltua tietoa.

Article 6

Classified Contracts

1. Upon request, the Competent Security Authority of the Receiving Party shall inform the Competent Security Authority of the Originating Party whether a proposed contractor of the Receiving Party has been issued a national Facility Security Clearance corresponding to the required security classification level. If the contractor does not hold a Facility Security Clearance, the Competent Security Authority of the Originating Party may request that the contractor be security cleared by the Competent Security Authority of the Receiving Party.

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

3. To allow adequate security supervision and control a Classified Contract, referred to in Annex 1 to this Agreement, shall contain appropriate security provisions, including a classification guide. A copy of the security provisions shall be forwarded to the Competent Security Authority of the Party under whose jurisdiction the contract is to be performed.

4. Representatives of the Competent Security Authorities of the Parties may visit each other upon request in order to analyse the efficiency of the measures adopted by a contractor for the protection of Classified Information involved in a Classified Contract.

7 artikla

Turvallisuusluokitellun tiedon välittäminen ja rekisteröinti

1. Osapuolet välittävät turvallisuusluokitellun tiedon toisilleen käyttäen suojattuja hallitusten välisiä kanavia tai muutoin siten kuin niiden toimivaltaiset turvallisuusviranomaiset keskenään sopivat.
2. Osapuolet vaihtavat keskenään turvallisuusluokkaan LUOTTAMUKSELLINEN tai sitä ylempään turvallisuusluokkaan kuuluvaa tietoa ja rekisteröivät sen asianmukaisesti kansallisia säädöksiä ja määräyksiä noudattaen.

Article 7

Transmission and registration of Classified Information

1. Classified Information shall be transmitted between the Parties through government-to-government secured channels or as otherwise agreed between their Competent Security Authorities.
2. Classified Information marked CONFIDENTIAL or higher exchanged between the Parties shall be duly registered according to national laws and regulations.

8 artikla

Turvallisuusluokitellun tiedon kääntäminen, kopiointi ja hävittäminen

1. Kaikkiin turvallisuusluokitellun tiedon kopioihin ja käännöksiin tehdään asianmukaiset turvallisuusluokitusmerkinnät, ja ne suojataan kuten alkuperäinen turvallisuusluokiteltu tieto. Käännöksiä tehdään ja kopioita otetaan ainoastaan viralliseen tarkoitukseen tarvittava vähimmäismäärä.
2. Kaikkiin käännöksiin tehdään asianmukainen käännöskielinen merkintä siitä, että käännökset sisältävät luovuttavan osapuolen turvallisuusluokiteltua tietoa.
3. Turvallisuusluokkaan SALAINEN tai sitä ylempään turvallisuusluokkaan kuuluvaa tietoa saa kääntää tai kopioida ainoastaan luovuttavan osapuolen kirjallisella suostumuksella.
4. Turvallisuusluokkaan SALAINEN tai sitä ylempään turvallisuusluokkaan kuuluvaa tietoa ei saa hävittää ilman luovuttavan osapuolen kirjallista ennakkosuostumusta. Tieto palautetaan luovuttavalle osapuolelle sen jälkeen, kun osapuolet katsovat, ettei sitä enää tarvita.
5. Turvallisuusluokkaan LUOTTAMUKSELLINEN kuuluva tieto hävitetään sen jälkeen, kun sitä ei enää katsota tarvittavan.
6. Jos kriisitilanne estää tämän sopimuksen mukaisesti luovutetun turvallisuusluokitellun tiedon suojaamisen, tieto hävitetään välittömästi. Vastaanottava osapuoli ilmoittaa turvallisuusluokitellun tiedon hävittämisestä

Article 8

Translation, reproduction and destruction of Classified Information

1. All reproductions and translations of Classified Information 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. All translations shall contain a suitable annotation, in the language of translation, indicating that they contain Classified Information of the Originating Party.
3. Classified Information marked SECRET or higher shall be translated or reproduced only upon the written consent of the Originating Party.

4. Classified Information marked SECRET or higher 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 Parties.

5. Classified Information marked CONFIDENTIAL shall be destroyed after it is no longer considered necessary.
6. If a crisis situation makes it impossible to protect Classified Information provided under this Agreement, the Classified Information shall be destroyed immediately. The Receiving Party shall notify the Competent

luovuttavan osapuolen toimivaltaiselle turvallisuusviranomaiselle mahdollisimman pian.

9 artikla

Vierailut

1. Vierailuihin, joihin liittyy mahdollisuus päästä turvallisuusluokiteltuun tietoon, vaaditaan isäntäosapuolen toimivaltaisen turvallisuusviranomaisen kirjallinen ennakkolupa. Vierailijoille sallitaan pääsy turvallisuusluokiteltuun tietoon ainoastaan, jos

a) vieraat lähettävän osapuolen toimivaltainen turvallisuusviranomainen on antanut heille luvan pyydettyyn yhteen tai useampaan vierailuun,

b) heille on annettu asianmukainen todistus henkilöturvallisuusselvityksestä, ja

c) heille on annettu lupa ottaa vastaan turvallisuusluokiteltua tietoa isäntäosapuolen kansallisten säädösten ja määräysten mukaisesti.

2. Vierailupyynnön esittävän osapuolen asianomainen toimivaltainen turvallisuusviranomainen ilmoittaa suunnitellusta vierailusta isäntäosapuolen asianomaiselle toimivaltaiselle turvallisuusviranomaiselle tämän artiklan määräysten mukaisesti sekä varmistaa, että isäntäosapuolen toimivaltainen turvallisuusviranomainen saa vierailupyynnön vähintään 14 päivää ennen vierailun ajankohtaa. Kiireellisissä tapauksissa toimivaltaiset turvallisuusviranomaiset voivat sopia lyhyemmästä ajasta. Vierailupyynnön on sisällettävä tämän sopimuksen liitteessä 2 tarkoitetut tiedot.

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

10 artikla

Turvallisuusyhteistyö

1. Tämän sopimuksen täytäntöön panemiseksi kansalliset turvallisuusviranomaiset antavat toisilleen tiedoksi asianomaiset turvallisuusluokitellun tiedon suojaamista koskevat kansalliset säädöksensä ja määräyksensä sekä niiden mahdolliset myöhemmät muutokset.

2. Varmistaakseen läheisen yhteistyön tämän sopimuksen täytäntöönpanossa toimival-

Security Authority of the Originating Party about the destruction of the Classified Information as soon as possible.

Article 9

Visits

1. Visits entailing a possibility of access to Classified Information require prior written authorisation from the Competent Security Authority of the host Party. Visitors shall only be allowed access where they have been:

a) authorised by the Competent Security Authority of the sending Party to conduct the required visit or visits,

b) granted an appropriate Personnel Security Clearance, and

c) authorised to receive Classified Information in accordance with the national laws and regulations of the host Party.

2. The relevant 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 request for visit at least 14 days before the visit takes place. In urgent cases the Competent Security Authorities may agree on a shorter period. The request for visit shall contain the information referred to in Annex 2 to this Agreement.

3. The validity of authorisations for recurring visits shall not exceed twelve (12) months.

Article 10

Security co-operation

In order to implement this Agreement the National Security Authorities shall notify each other of their relevant national laws and regulations regarding the protection of Classified Information as well as of any subsequent amendments thereto.

2. In order to ensure close co-operation in the implementation of this Agreement the

taiset turvallisuusviranomaiset neuvottelevat keskenään. Ne antavat pyynnöstä toisilleen tietoa turvallisuusluokitellun tiedon suojaamista koskevista kansallisista turvallisuusnormeistaan, menettelyistään ja käytännöistään. Tätä tarkoitusta varten toimivaltaiset turvallisuusviranomaiset voivat tehdä keskinäisiä vierailuja.

3. Toimivaltaiset turvallisuusviranomaiset avustavat pyynnöstä toisiaan kansallisten säädösten ja määräysten mukaisesti turvallisuusselvitysten tekemisessä.

4. Kansalliset turvallisuusviranomaiset ilmoittavat viipymättä toisilleen asianomaisten turvallisuusselvityksistä annettujen todistusten muutoksista.

5. Tätä sopimusta ei sovelleta turvallisuusluokitellun tiedon vaihtamiseen osapuolten tiedustelupalvelujen ja lainvalvontaviranomaisten (esimerkiksi poliisin) välillä.

Competent Security Authorities shall consult each other. On request, they shall provide each other with information about their national security standards, procedures and practices for the protection of Classified Information. To this aim the Competent Security Authorities may visit each other.

3. On request, Competent Security Authorities shall, in accordance with national laws and regulations, assist each other in carrying out security clearance procedures.

4. The National Security Authorities shall promptly inform each other about changes in relevant security clearance certificates.

5. This Agreement does not apply to the exchange of Classified Information between the intelligence services and the law enforcement agencies (e.g. the police) of the two Parties.

11 artikla

Tietoturvaloukkaus

1. Kumpikin osapuoli ilmoittaa viipymättä toiselle osapuolelle epäillystä tai todetusta turvallisuusluokiteltuun tietoon kohdistuvasta tietoturvaloukkauksesta.

2. Kumpikin osapuoli tutkii tapauksen viipymättä kansainvälisen oikeuden ja kansallisen lainkäyttövaltansa rajoissa. Toinen osapuoli tekee tarvittaessa tutkintayhteistyötä toimivaltaisen osapuolen kanssa.

3. Kumpikin osapuoli toteuttaa kansainvälisen oikeuden ja kansallisen lainkäyttövaltansa rajoissa kaikki mahdolliset asianmukaiset kansallisten säädöstensä ja määräystensä mukaiset toimet rajoittaakseen tämän artiklan 1 kohdassa tarkoitettujen tietoturvaloukkausten seurauksia ja estääkseen tietoturvaloukkausten jatkumisen. Toiselle osapuolelle ilmoitetaan tutkinnan ja toteutettujen toimien tuloksista.

Article 11

Breach of Security

1. Each Party shall immediately notify the other Party of any suspected or discovered Breach of Security of Classified Information.

2. Each Party shall, within the limits of the international law and its domestic jurisdiction, investigate the incident without delay. The other Party shall, if required, cooperate in the investigation of the Party with jurisdiction.

3. Each Party shall, within the limits of the international law and its domestic jurisdiction undertake all possible appropriate measures under its national laws and regulations so as to limit the consequences of breaches referred to in Paragraph 1 of this Article and to prevent further breaches. The other Party shall be informed of the outcome of the investigation and of the measures undertaken.

12 artikla

Kustannukset

Kumpikin osapuoli vastaa omista kustannuksistaan, jotka niille aiheutuvat tästä sopi-

Article 12

Costs

Each Party shall bear its own costs incurred in the course of implementing its obligations

muksesta johtuvien velvoitteiden täyttämisestä.

13 artikla

Riitojen ratkaiseminen

Kaikki osapuolten väliset riidat, jotka koskevat tämän sopimuksen tulkintaa tai soveltamista, ratkaistaan yksinomaan osapuolten välisin neuvotteluin.

14 artikla

Loppumääräykset

1. Osapuolet ilmoittavat toisilleen, kun tämän sopimuksen voimaantulon edellyttämät kansalliset toimet on toteutettu. Sopimus tulee voimaan toiseksi seuraavan kuukauden ensimmäisenä päivänä sen jälkeen, kun jälkimmäinen ilmoitus on otettu vastaan.

2. Tämä sopimus on voimassa toistaiseksi. Sopimusta voidaan muuttaa osapuolten keskinäisellä kirjallisella suostumuksella. Osapuoli voi milloin tahansa ehdottaa tämän sopimuksen muuttamista. Jos jompikumpi osapuoli sitä ehdottaa, osapuolet aloittavat neuvottelut sopimuksen muuttamisesta.

3. Osapuoli voi irtisanoa tämän sopimuksen ilmoittamalla asiasta kirjallisesti toiselle osapuolelle diplomaattiteitse kuuden (6) kuukauden irtisanomisaikaa noudattaen. Jos sopimus irtisanotaan, sopimuksen perusteella jo luovutettua ja sen perusteella syntyvää turvallisuusluokiteltua tietoa käsitellään sopimuksen määräysten mukaisesti niin kauan kuin se on tarpeen kyseisen tiedon suojaamiseksi.

Tämä sopimus korvaa Bernissä 17 päivänä maaliskuuta 1994 allekirjoitetun Suomen puolustusministeriön ja Sveitsin puolustusministeriön yhteisymmärryspöytäkirjan turvallisuusluokitellun tiedon vaihtamisesta.

Tämän vakuudeksi asianmukaisesti valtuutetut osapuolten edustajat ovat allekirjoittaneet tämän sopimuksen

Solothurmissa 28 päivänä tammikuuta 2014.

under this Agreement.

Article 13

Resolution of disputes

Any dispute between the Parties on the interpretation or application of this Agreement shall be resolved exclusively by means of consultations between the Parties.

Article 14

Final provisions

1. The Parties shall notify each other of the completion of the national measures necessary for the entry into force of this Agreement. The Agreement shall enter into force on the first day of the second month following the receipt of the later notification.

2. This Agreement shall be in force until further notice. The Agreement may be amended by the mutual, written consent of the Parties. Either Party may propose amendments to this Agreement at any time. If one Party so proposes, the Parties shall begin consultations on amending the Agreement.

3. Either Party may terminate this Agreement by written notification delivered to the other Party through diplomatic channels, observing a period of notice of six (6) months. If the Agreement is terminated, any Classified Information already provided and any Classified Information arising under the Agreement shall be handled in accordance with the provisions of the Agreement for as long as necessary for the protection of the Classified Information.

The present Agreement replaces the Memorandum of Understanding between the Ministry of Defence of Finland and the Ministry of Defence of Switzerland concerning the Exchange of Classified Information, signed in Berne on 17th March 1994.

In witness whereof the duly authorised representatives of the Parties have signed this Agreement,

in Solothurm on the 28th day of January, 2014.

kahtena kappaleena englannin kielellä.

Suomen tasavallan hallituksen puolesta

Alpo Rusi
Suomen tasavallan Sveitsin-suurlähettiläs

Sveitsin liittoneuvoston puolesta

Urs Freiburghaus
Tietoturvallisuus- ja toimitilasuojausosaston johtaja

in two duplicates in the English language.

For the Government of the Republic of Finland

Alpo Rusi
Ambassador of the Republic of Finland to Switzerland

For the Swiss Federal Council

Urs Freiburghaus
Head of Directorate for Information Security and Facility Protection

Liite 1

Turvallisuusluokitellut sopimukset

Tämän sopimuksen 6 artiklassa tarkoitettujen turvallisuusluokiteltujen sopimusten on-sisällettävä seuraavat tiedot:

1. menettely, jolla käyttäjälle annetaan oikeus käsitellä turvallisuusluokiteltua tietoa
2. säädökset ja määräykset, jotka muodostavat perustan turvallisuusluokitellun tiedon käytölle
3. vaadittava turvallisuusluokka
4. turvallisuusluokitellun tiedon käyttöä koskevat rajoitukset
5. turvallisuusluokitellun tiedon välittämistä koskevat yksityiskohtaiset säännöt
6. turvallisuusluokitellun tiedon käsittelyä koskevat yksityiskohtaiset säännöt
7. turvallisuusluokitellun tiedon merkitseminen ja sen käytännön vaikutukset
8. tiedot henkilöistä, mukaan lukien alihankkijat, joilla on oikeus saada turvallisuusluokiteltua tietoa, ja tiedon saannin edellytykset
9. turvallisuusluokitellun tiedon suojaamisaikaa koskevat vaatimukset
10. menettely turvallisuusluokitellun tiedon hävittämiseksi tai palauttamiseksi.

Annex 1

Classified Contracts

Classified Contracts referred to in Article 6 of this Agreement shall contain the following information:

1. procedure entitling a user to handle Classified Information
2. laws and regulations forming the base for the use of Classified Information
3. classification level required
4. limitations on the use of Classified Information
5. modalities of transmission of Classified Information
6. modalities of handling Classified Information
7. marking of Classified Information and practical consequences thereof
8. specifications of the persons, including sub-contractors, entitled to receive Classified Information and the conditions therefore
9. requirements for the period of protecting Classified Information
10. procedure for destroying or returning Classified Information

Liite 2

Vierailupyyntö

Tämän sopimuksen 9 artiklassa tarkoitettujen vierailupyyntöjen on sisällettävä seuraavat tiedot:

1. vierailijan suku- ja etunimi, syntymäpaikka ja -aika/alkuperä ja kansallisuus; vierailijan asema ja tiedot hänen edustamastaan työnantajasta; tiedot hankkeesta, johon vierailija osallistuu, ja vierailijan passin tai muun henkilöllisyystodistuksen numero

2. vahvistus vierailun tarkoitusta vastaavasta vierailijan henkilöturvallisuusselvityksestä

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

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

5. vierailun kohteena olevan toimipaikan tai laitoksen nimi, osoite, puhelin- ja faksinumero sekä sähköpostiosoite ja yhteyshenkilö, tiedot aiemmista yhteyksistä sekä muut vierailun tai vierailujen perusteltavuuden määrittämiseksi tarpeelliset tiedot

6. päiväys sekä vierailupyynnön lähettävän toimivaltaisen turvallisuusviranomaisen allekirjoitus ja leima.

Annex 2

Request for visit

Requests for visit referred to in Article 9 of this Agreement shall contain the following information:

1. the visitor's family name, first name, place and date of birth/origin 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, and the visitor's passport number or other identity document number;

2. confirmation of Personnel Security Clearance of the visitor in accordance with the purpose of the visit;

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

4. 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;

5. the name, address, phone and fax number, e-mail and point of contact of the establishment or facility to be visited, previous contacts and any other information useful for determining the justification for the visit or visits;

6. the date, signature and seal of the sending Competent Security Authority.