Hallituksen esitys eduskunnalle turvallisuusluokitellun tiedon vastavuoroisesta suojaamisesta Suomen ja Itävallan välillä tehdyn sopimuksen hyväksymiseksi ja voimaansaattamiseksi

ESITYKSEN PÄÄASIALLINEN SISÄLTÖ

Esityksessä ehdotetaan, että eduskunta hyväksyisi Suomen ja Itävallan välisen sopimuksen turvallisuusluokitellun tiedon vastavuoroisesta suojaamisesta sekä lain, jolla saatetaan voimaan sopimuksen lainsäädännön alaan kuuluvat määräykset.

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

Osapuolet ilmoittavat toisilleen kun sopimuksen voimaantulon edellyttämät kansalliset toimet 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.

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 (tiedon saatavuus tarvittaessa). Tietoturvallisuuden varmistamiseksi käytetään erilaisia keinoja, joita 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, sekä Suomen luovuttamien aineistojen suojaamisesta. Kansainvälinen tietoturvallisuusyhteistyö, johon Suomikin osallistuu, käsittää perinteisesti diplomaattiseen toimintaan samoin kuin puolustushallintojen väliseen yhteistyöhön liittyvän ei-julkisen tiedonvaihdon suojaamisen. Valtioiden välillä vaihdettavien tietojen lisäksi kansainvälisillä tietoturvallisuusvelvoitteilla on kasvava merkitys myös taloudellisessa, teollisessa sekä teknologisessa yhteistyössä, joissa puitteissa kaupalliset 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. Tietoturvallisuussopimus luo yrityksille sopimuskehikon hankinnan toteuttamiselle, jotta suomalaiset yritykset voisivat osallistua tällaisten alojen hankintoihin.

Suomi on tehnyt kahdenvälisen tietoturvallisuussopimuksen seuraavien sopimuskumppaneiden kanssa:

- Euroopan Avaruusjärjestö (ESA) (SopS 94 ja 95/2004)
- Saksa (SopS 96 ja 97/2004)
- Ranska (SopS 66 ja 67/2005)
- Slovakia (SopS 116 ja 117/2007)
- Viro (SopS 12 ja 13/2008)
- Italia (SopS 23 ja 24/ 2008)
- Latvia (SopS 33 ja 34/2008)
- Puola (SopS 46 ja 47/2008)
- Eurooppalainen puolustusmateriaaliyhteistyöjärjestö (OCCAR) (SopS 109 ja 110/2008)
- Bulgaria (SopS 116 ja 117/2008)
- Slovenia (SopS 22 ja 23/2009)
- Tšekki (SopS 53 ja 54/2009)
- Espanja (SopS 38 ja 39/2010)
- Pohjois-Atlantin liitto (Nato) (SopS 7 ja 8/2013)
- Amerikan yhdysvallat (SopS 41 ja 42/2013)
- Iso-Britannia (SopS 49 ja 50/2013)
- Luxemburg (SopS 59 ja 60/2013)
- Sveitsi (SopS 88 ja 89/2014)
- Kroatia (SopS 38 ja 39/2015)

- Israel, jonka kanssa on tehty soveltamisalaltaan suppeampi sopimus puolustus- tai turvallisuushallintojen kesken välitetystä turvallisuusluokitellusta tiedosta (SopS 34 ja 35/2012).

Tietoturvallisuusalan monenkeskistä yleissopimusta ei ole olemassa. Edellä sanotusta poikkeuksena on Tanskan, Suomen, Islannin, Norjan ja Ruotsin välillä turvallisuusluokitellun tiedon vastavuoroisesta suojaamisesta ja vaihtamisesta tehty yleinen turvallisuussopimus (SopS 11 ja 12/2013). EU:n jäsenvaltioiden välillä tehty sopimus turvallisuusluokitellun tiedon suojaamisesta (SopS 76 ja 77/2015) tuli voimaan 1 päivänä joulukuuta 2015. EU:n jäsenvaltioiden välillä tehdyn sopimuksen yhtenä tavoitteena on luoda järjestelmä EU:n edun vuoksi vaihdettavan kansallisen turvallisuusluokitellun tiedon suojaamiseksi silloin, kun jäsenvaltiot eivät ole tehneet kahdenvälistä tietoturvallisuussopimusta. Sopimuksen määräykset eivät kuitenkaan ole yhtä kattavia kuin yleisen kahdenvälisen tietoturvallisuussopimuksen vastaavat. Näin ollen se ei poista tarvetta tehdä kahdenvälisiä tietoturvallisuussopimuksia EU:n jäsenvaltioiden välillä.

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

Lakia kansainvälisistä tietoturvallisuusvelvoitteista (588/2004) sovelletaan erityissuojattaviin tietoaineistoihin. Näillä tarkoitetaan 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. 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 erityissuojattaviin tietoaineistoihin sisältyviä tai tällaisista saatavissa olevia tietoja. Lakia ei sovelleta pelkästään Suomen kansallista tietoa sisältävien asiakirjojen tai niiden osien salassapitoon tai luokitukseen.

Laissa on säännökset henkilöturvallisuusselvitystodistuksen (Personnel Security Clearance Certificate, PSCC) ja yritysturvallisuusselvitystodistuksen (Facility Security Clearance Certificate, FSCC) myöntämisestä. Henkilö- tai yritysturvallisuusselvityksen laatineen viranomaisen on salassapitosäännösten estämättä toimitettava todistuksen antamista ja siihen liittyvää harkintaa varten kansalliselle turvallisuusviranomaiselle tieto kaikista selvityksen laadinnassa ilmi tulleista selvityksen kohdetta koskevista seikoista (11 §:n 1 mom. ja 12 §:n 1 mom.).

Todistuksen antamista koskevaan arvioon sekä todistuksen voimassaoloon ja peruuttamiseen sovelletaan turvallisuusselvityslakia (kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 11 §:n 2 mom. ja 12 §:n 2 mom.). Jos kansallinen turvallisuusviranomainen kieltäytyy antamasta henkilö- tai yritysturvallisuusselvitystodistusta, sen tulee ilmoittaa syyt tähän selvi-

tyksen hakijalle ja sen kohteelle annettavassa kirjallisessa päätöksessä (kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 11 §:n 3 mom. ja 12 §:n 3 mom.). Muutoksenhausta säädetään lain 20 a §:ssä.

Lain suhde julkisuuslainsäädäntöön

Kansainvälisistä tietoturvallisuusvelvoitteista annettuun lakiin sisältyy kansallisten asiakirjojen tietoturvallisuudesta annetuista säännöksistä poikkeavia säännöksiä. Laissa on kuitenkin yleinen viittaussäännös julkisuuslakiin (3 §:n 1 mom.). Niiltä osin kuin suomalaisten viranomaisten asiakirjoihin sisältyy muita kuin kansainvälisten tietoturvallisuusvelvoitteiden piiriin kuuluvia tietoja kansainvälisestä yhteistyöstä, on sovellettava julkisuuslain (621/1999) ja sen nojalla annettuja säännöksiä. Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 3 §:n 2 momentin mukaan julkisuuslakiin tai muuhun lakiin perustuvan pyynnön saada tieto erityissuojattavasta tietoaineistosta käsittelee ja ratkaisee se viranomainen, jolle tietoaineisto on toimitettu taikka jonka käsiteltäväksi asia kokonaisuudessaan kuuluu.

Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain säännöksiä sovelletaan niin kauan kuin se turvallisuusluokituksen perusteena olevan yleisen edun vuoksi on tarpeen silloinkin, kun sopimus tai säädös, johon säännösten soveltaminen perustuu, ei enää ole voimassa (15 §). Salassapitovelvollisuuden lakkaamisesta on voimassa mitä julkisuuslaissa säädetään. Julkisuuslain 31 §:n 2 momentin mukaan viranomaisen asiakirjan salassapitoaika on 25 vuotta, jollei toisin ole säädetty. Julkisuuslain 31 §:n 3 momentin mukaan asiakirjan salassapito voi jatkua 25 vuoden jälkeenkin, mikäli asiakirja sisältää kansainvälisistä tietoturvallisuusvelvoitteista annetun lain mukaan turvallisuusluokiteltua tietoa, ja mikäli tiedon antaminen asiakirjasta aiheuttaisi julkisuuslain 24 §:n 1 momentin 2, 7, 8 tai 10 kohdassa tarkoitetun haittaseurauksen. Tällaiset asiakirjat tulevat julkisuuslain 31 §:n 3 momentin mukaan julkisiksi kun turvallisuusluokitus on kumottu.

Lain soveltaminen elinkeinonharjoittajiin

Kansainvälisistä tietoturvallisuusvelvoitteista annettua 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 1 momentin 3 kohta).

Elinkeinonharjoittajalla ja tämän palveluksessa tai toimeksiannosta toimivalla on erityissuojattavia tietoaineistoja koskeva salassapitovelvollisuus, velvollisuus käyttää tällaista tietoaineistoa vain siihen tarkoitukseen, johon se on annettu sekä velvollisuus pitää huolta siitä, että tietoaineistoon on pääsy vain niillä, jotka tarvitsevat tietoa tehtävän hoitamisessa (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

Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 4 §:ssä on säännökset niistä viranomaisista, jotka huolehtivat kansainvälisten tietoturvallisuusvelvoitteiden hoitamisesta. Kansallisena turvallisuusviranomaisena *(National Security Authority, NSA)* kansainvälisten tietoturvallisuusvelvoitteiden toteuttamiseen liittyvissä tehtävissä toimii ulkoministeriö. Puolustusministeriö, pääesikunta, Suojelupoliisi ja Viestintävirasto toimivat kansainvälisissä tietoturvallisuusvelvoitteissa tarkoitettuina määrättyinä turvallisuusviranomaisina *(Designated Security Authority, DSA)*.

Tietojen salassapito ja käytön sääntely

Erityissuojattava tietoaineisto on pidettävä salassa, jollei kansainvälisestä tietoturvallisuusvelvoitteesta muuta johdu (kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 6 §:n 1 mom.). Salassapitovelvollisuus koskee myös elinkeinonharjoittajaa tämän ollessa osapuolena turvallisuusluokitellussa sopimuksessa. Suomen tekemissä kahdenvälisissä sopimuksissa, jotka koskevat eri maiden viranomaisten välistä salassa pidettävien tietojen vaihtoa ja suojaamista, 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

Kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa säädetään velvollisuudesta merkitä erityissuojattavaan tietoaineistoon sen turvallisuusluokka. Erityissuojattavaan tietoaineistoon tehty merkintä turvallisuusluokasta osoittaa, minkälaisia tietoturvallisuusvaatimuksia sen käsittelyssä on noudatettava (8 §). Mitä korkeampaan turvallisuusluokkaan aineisto kuuluu, sitä tiukempia tietoturvallisuustoimenpiteitä edellytetään. Laissa on yleinen velvoite toteuttaa tietoaineiston käsittelyssä sen turvallisuusluokkaa koskevia käsittelymääräyksiä sekä valtuus säätää erityissuojattavan tietoaineiston käsittelyssä noudatettavista 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 kansainvälisiä tietoturvallisuusvelvoitteita toteutettaessa.

Erityissuojattava tietoaineisto on kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 10 §:n mukaan säilytettävä tiloissa, joissa asiakirjojen ja materiaalien sekä niihin sisältyvien tietojen suojaamisesta voidaan huolehtia kansainvälisessä tietoturvallisuusvelvoitteessa edellytetyllä tavalla. Tilojen turvallisuusvaatimuksista on säädetty tietoturvallisuusasetuksen 14 §:ssä.

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 kansainvälisessä tietoturvallisuusvelvoitteessa tätä edellytetään (lain 6 §:n 3 mom.). Sama koskee myös 1 §:n 2 momentissa tarkoitettua elinkeinonharjoittajaa.

2.2 Turvallisuusselvityslaki

Lain tarkoitus ja soveltamisala

Turvallisuusselvityslain (726/2014) tarkoituksena on parantaa mahdollisuuksia ennakolta ehkäistä toimintaa, joka voi vahingoittaa valtion turvallisuutta, maanpuolustusta, Suomen kansainvälisiä suhteita, yleistä turvallisuutta tai muuta niihin verrattavaa yleistä etua taikka erittäin merkittävää yksityistä taloudellista etua taikka edellä tarkoitettujen etujen suojaamiseksi toteutettavia turvallisuusjärjestelyjä (1 §).

Laissa säädetään henkilö- ja yritysturvallisuusselvityksen laadinnassa noudatettavasta menettelystä. Laki sisältää säännökset turvallisuusselvityksen laatimisen edellytyksistä sekä sitä laadittaessa käytettävistä tiedoista, selvityksen kohteen suostumuksesta ja tiedonsaantioikeuksista, selvityksen hakijan ja selvityksen kohteen tiedonantovelvollisuuksista sekä turvallisuusselvityksen ja sen perusteella annetun todistuksen voimassaolosta ja todistuksen peruuttamisesta, sekä henkilörekisterien yhdistämisestä selvityksen kohteen nuhteettomuuden ja luotettavuuden seuraamiseksi ja sen johdosta suoritettavista toimenpiteistä (2 §).

Yksityisyyden suojan perusoikeusluonteen vuoksi turvallisuusselvitysmenettely on tarkan muotosidonnaista. Turvallisuusselvitys voidaan tehdä vain selvityksen kohteen etukäteen antaman kirjallisen suostumuksen perusteella (5 §).

Henkilöstöturvallisuus

Henkilöturvallisuusselvityksellä tarkoitetaan turvallisuusselvityslain 3 §:n 1 momentin 1 kohdan mukaisesti henkilön nuhteettomuuden tai luotettavuuden varmistamiseksi turvallisuusselvityslaissa säädetyllä tavalla laadittavaa selvitystä henkilön taustasta. Lain 23 §:n mukaan henkilöturvallisuusselvitys tehdään tarkistamalla henkilöä koskevat rekisteritiedot lain 4 luvussa säädetyllä tavalla sekä tarvittaessa selvityksen kohdetta haastattelemalla hänen yleisistä olosuhteistaan, ulkomailla oleskelustaan, ulkomaansidonnaisuuksistaan ja hänen suhteistaan muiden maiden kansalaisiin sekä muista sellaisista seikoista, joilla on erityistä merkitystä arvioitaessa hänen riippumattomuuttaan ja luotettavuuttaan muutoinkin selvityksen perustana olevan tehtävän kannalta.

Lain 14 §:n mukaan henkilöturvallisuusselvitys voidaan laatia suppeana, perusmuotoisena tai laajana. Turvallisuusselvitys tehdään laissa määritellyissä tapauksissa, kuten silloin, kun Suomea sitova valtiosopimus tai muu kansainvälinen velvoite edellyttää turvallisuusselvityksen tekemistä tai sen perusteella laaditun todistuksen esittämistä.

Jokaisella on oikeus saada tieto siitä, onko hänestä tehty turvallisuusselvitys tiettyä tehtävää varten. Selvityksen kohteella on myös oikeus pyynnöstä saada toimivaltaiselta viranomaiselta turvallisuusselvityksen tiedot. Tiedonsaantioikeus ei kuitenkaan koske sellaisesta rekisteristä peräisin olevaa tietoa, johon rekisteröidyllä ei ole tarkastusoikeutta (6 §).

Turvallisuusselvitysmenettelyssä käytetyt rekisterit on laissa lueteltu tyhjentävästi. Turvallisuusselvityksessä voidaan käyttää myös tiettyjä ulkomaan viranomaisen rekistereihin talletettuja tietoja (25 §).

Turvallisuusselvityslain 43 §:n 2 momentin mukaan kansallinen turvallisuusviranomainen antaa kansainvälisen tietoturvallisuusvelvoitteiden toteuttamiseksi tarpeellisen henkilöturvalli-

suusselvitystodistuksen siten kuin kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa säädetään.

Yritysturvallisuus

Turvallisuusselvityslain 33 §:ssä määritellään yritysturvallisuusselvityksen hakemiseen oikeutetut ja 36 §:ssä yritysturvallisuusselvityksen laatimisen edellytykset. Lain 37 §:ssä on lueteltu yritysturvallisuusselvityksissä käytettävät tietolähteet ja lain 38 § koskee yritysturvallisuusselvitysasian käsittelyä. Yritysturvallisuusselvitystä laadittaessa selvitetään hakemuksessa esitettyjen tietojen ja 37 §:ssä tarkoitettujen tietolähteiden sekä yrityksen toimitilojen ja tietojärjestelmien tarkastuksen avulla, miten yritys huolehtii tietojen suojaamisesta, asiattoman pääsyn estämisestä tiloihin ja henkilöstön koulutuksesta (38 §:n 1 mom.). Yritysturvallisuusselvitys voidaan tehdä myös osittaisena, jos se on tarpeen kansainvälisen tietoturvallisuusvelvoitteen toteuttamiseksi tai muutoin perusteltua (38 §:n 3 mom). Kansainvälisesti käytössä on kolme yritysturvallisuusselvityksen muotoa: 1) nk. rajattu yritysturvallisuusselvitys, ”FSC without safeguards”, joka ei sisällä yrityksen toimitilojen tai tietojärjestelmien tarkastuksia, 2) yritysturvallisuusselvitys ”FSC with safeguards”, joka sisältää toimitilojen tarkastukset ja 3) yritysturvallisuusselvitys ”FSC with safeguards including Communications and Information Systems”, joka sisältää toimitilojen ja tietojärjestelmien tarkastukset.

Selvityksen laatii turvallisuusselvityslain 9 §:n mukaan Suojelupoliisi. Pääesikunta huolehtii yritysturvallisuusselvityksen laatimisesta kuitenkin silloin, kun kysymys on yrityksestä, joka hoitaa tai jonka on tarkoitus hoitaa puolustusvoimien antamaa tehtävää, taikka yrityksestä, joka liittyy puolustusvoimien hankintoihin. Viestintäviraston tehtävänä on huolehtia yrityksen tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista.

Toimivaltainen viranomainen voi yritysturvallisuusselvitystä ja sen perusteella annettavaa todistusta laatiessaan turvallisuusselvityslain 40 §:n mukaan edellyttää yritykseltä sitoumusta, jonka mukaan elinkeinonharjoittaja sitoutuu huolehtimaan tietoturvallisuustason säilyttämisestä sekä ilmoittamaan muutoksista, joilla on siihen vaikutuksia sekä antamaan tietoturvallisuustason säilyttämisen valvomiseksi viranomaiselle luvan päästä yrityksen tiloihin sekä antamaan seurannassa tarvittavia tietoja.

Lain 46 §:n 2 momentin mukaan kansallinen turvallisuusviranomainen antaa kansainvälisen tietoturvallisuusvelvoitteiden toteuttamiseksi tarpeellisen yritysturvallisuusselvitystodistuksen siten kuin kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa säädetään.

3 Esityksen tavoitteet ja keskeiset ehdotukset

Esityksen tavoitteena on hankkia eduskunnan hyväksyntä sopimukselle. Sopimuksen tavoitteena on varmistua siitä, että Suomen Itävaltaan luovuttamaa turvallisuusluokiteltua tietoa suojataan ja käsitellään asianmukaisesti. Sopimuksen tavoitteena on myös edistää Suomen mahdollisuuksia vastaanottaa Itävallan turvallisuusluokiteltua tietoa ja parantaa maiden välistä yhteistyötä tietoturvallisuuden alalla. Lisäksi sopimuksen tarkoituksena on turvata suomalaisten yritysten mahdollisuudet osallistua sellaisiin kansainvälisiin sekä Suomen ja Itävallan välisiin hankkeisiin, joiden toteuttaminen saattaa edellyttää turvallisuusluokiteltujen tietojen vaihtoa. Esitys sisältää myös ehdotuksen niin sanotuksi blankettilaiksi, jolla saatetaan voimaan sopimuksen lainsäädännön alaan kuuluvat määräykset.

4 Esityksen vaikutukset

4.1 Vaikutukset kansalaisiin

Sopimuksen voimaansaattamisen myötä Itävallasta 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 Itävallan välisen sopimuksen mukaisia erityissuojattavia tietoaineistoja ovat aineistot, joita Itävalta pitää salassa pidettävinä ja jotka se on määritellyt ja merkinnyt korkean tietoturvallisuuden tasoa edellyttäviksi. Sopimuksen 5 artiklassa määrätään turvallisuusluokitellun tiedon suojaamisesta ja salassapidosta. Sopimuksen 5 artiklan 2 kohdan mukaan sopimuksen 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 Itävallan 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 kansainvälisistä tietoturvallisuusvelvoitteista annetun lain soveltamisessa julkisuuslain sijaan 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 epäselvyyttä luokituksen oikeellisuudesta tai siitä, mitkä asiakirjassa olevat tiedot ovat johtaneet luokitusmerkintään, viranomaisen on otettava yhteyttä asiakirjan laatineeseen osapuoleen.

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

Henkilöstöturvallisuus on keskeinen tietoturvallisuuden osa-alue. Koska jo kansainvälisistä tietoturvallisuusvelvoitteista annettu laki edellyttää turvallisuusselvityslain 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 Itävallan turvallisuusluokiteltuihin tietoihin. Vastaavasti sopimus antaa itävaltalaisille 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 Itävallassa 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.

Sopimuksen turvallisuusyhteistyötä koskevan 10 artiklan 4 kohdan mukaisesti turvallisuusviranomaiset avustavat pyynnöstä toisiaan turvallisuusselvityksiin liittyvissä menettelyissä kansallisten säädösten ja määräysten mukaisesti.

5 Asian valmistelu

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

YKSITYISKOHTAISET PERUSTELUT

1 Sopimuksen sisältö ja suhde Suomen lainsäädäntöön

1 artikla. *Tarkoitus ja soveltamisala*. Artiklassa määritellään sopimuksen tarkoitukseksi varmistaa sellaisen turvallisuusluokitellun tiedon suojaaminen, jota vaihdetaan tai tuotetaan osapuolten välisessä yhteistyössä. Sopimusta ei sovelleta sellaisiin osapuolten välillä vaihdettaviin tietoihin, joita ei ole turvallisuusluokiteltu. Esimerkiksi poliisin tutkinta- ja tiedustelutietoihin ei Suomessa pääosin tehdä turvallisuusluokitusmerkintää.

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 luokitusmerkintä kansallisten säädösten ja määräysten mukaisesti. Edelleen turvallisuusluokitellulla tiedolla tarkoitetaan 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 2 kohdan erityissuojattavan tietoaineiston määritelmän kanssa.

Artiklan b) kohdan mukaan turvallisuusluokiteltu sopimus tarkoittaa sopimusta tai alihankintasopimusta, johon sisältyy tai liittyy turvallisuusluokiteltua tietoa. Kohta on sopusoinnussa kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 2 §:n 3 kohdan kanssa.

Artiklan c) kohdan mukaan luovuttavalla osapuolella tarkoitetaan sitä osapuolta, joka luovuttaa turvallisuusluokitellun tiedon tai jonka alaisuudessa turvallisuusluokiteltu tieto tuotetaan.

Artiklan d) kohdan mukaisesti vastaanottajalla tarkoitetaan sitä osapuolta sekä sen lainkäyttövaltaan kuuluvaa oikeushenkilöä tai luonnollista henkilöä, jolle luovuttava osapuoli luovuttaa turvallisuusluokitellun tiedon.

Artiklan e) kohdan mukaisesti toimivaltainen turvallisuusviranomainen tarkoittaa 3 artiklassa tarkoitettua kansallista turvallisuusviranomaista, määrättyä turvallisuusviranomaista tai muuta toimivaltaista elintä, joka on osapuolten kansallisten säädösten ja määräysten mukaisesti valtuutettu vastaamaan sopimuksen täytäntöönpanosta.

Artiklan f) kohdan mukaan tietoturvaloukkaus tarkoittaa kansallisten säädösten ja määräysten vastaista tekoa tai laiminlyöntiä, joka saattaa johtaa turvallisuusluokitellun tiedon menettämiseen tai vaarantumiseen.

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

Artiklan h) kohdan mukaan kolmas osapuoli tarkoittaa sellaista valtiota, joka ei ole tämän sopimuksen osapuoli, tai sellaista oikeushenkilöä tai luonnollista henkilöä, joka ei kuulu kummankaan osapuolen lainkäyttövaltaan.

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). Itävallassa kansalliseksi turvallisuusviranomaiseksi on nimetty Information Security Commission (NSA)/Federal Chancellery.

Artiklan 2 kohdan mukaan kansalliset turvallisuusviranomaiset antavat toisilleen tiedoksi mahdolliset muut toimivaltaiset turvallisuusviranomaiset (Competent Security Authorities, CSA), jotka vastaavat sopimuksen täytäntöönpanosta eri osin, sekä näiden viranomaisten myöhemmät muutokset. Nämä tiedoksiannot sisältävät myös kansallisten turvallisuusviranomaisten ja muiden toimivaltaisten turvallisuusviranomaisten yhteystiedot. Suomessa määrättyjä turvallisuusviranomaisia (Designated Security Authority, DSA) ovat kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 4 §:n mukaisesti puolustusministeriö, pääesikunta, Suojelupoliisi ja Viestintävirasto.

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 Itävallan turvallisuusluokituksen tasot vastaavat toisiaan. Korkein, ankarimpia tietoturvallisuustoimenpiteitä vaativa luokka on "ERITTÄIN SALAINEN / YTTERST HEMLIG" ("STRENG GEHEIM"). Suomessa tähän luokkaan luetaan kuuluviksi tiedot, joiden luvaton ilmitulo voi aiheuttaa erityisen suurta vahinkoa maanpuolustukselle, turvallisuudelle, kansainvälisille suhteille tai muille yleisille eduille. Toiseksi korkein turvallisuusluokka on "SALAINEN/HEMLIG" ("GEHEIM"). 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") jolla tarkoitetaan Suomessa tietoja, joiden luvaton ilmitulo voi aiheuttaa vahinkoa maanpuolustukselle, turvallisuudelle, kansainvälisille suhteille tai muille yleisille eduille. Neljänteen turvallisuusluokkaan "KÄYTTÖ RAJOITETTU / BEGRÄNSAD TILLGÅNG" ("EINGESCHRÄNKT") 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 mainitussa 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 turvallisuusluokitusmerkinnöistä on erityissäännös asetuksen 11 §:n 4 momentissa.

Artiklan 3 kohdan mukaan vastaanottava osapuoli varmistaa, ettei turvallisuusluokituksia muuteta tai kumota, ellei luovuttava osapuoli anna siihen kirjallista lupaa. Luovuttava osapuoli ilmoittaa viipymättä vastaanottajalle, jos välitetyn turvallisuusluokitellun tiedon turvallisuusluokkaa muutetaan tai se kumotaan.

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

Artiklan 1 kohdan mukaan osapuolet toteuttavat kaikki asianmukaiset toimet suojatakseen sopimuksessa tarkoitettua turvallisuusluokiteltua tietoa ja mahdollistavat tämän suojaamisen tarvittavan valvonnan. Osapuolet antavat saman kohdan mukaisesti tälle tiedolle samantasoisen suojan kuin omalle vastaavaan turvallisuusluokkaan kuuluvalle tiedolleen kansallisten säädöstensä ja määräystensä mukaisesti.

Artiklan 2 kohdan mukaan osapuolet eivät salli kolmansille osapuolille pääsyä turvallisuusluokiteltuun tietoon ilman luovuttavan osapuolen kirjallista ennakkosuostumusta. Kohta velvoittaa osapuolet noudattamaan luovuttajan suostumuksen periaatetta.

Artiklan 3 kohdan mukaan pääsy turvallisuusluokiteltuun tietoon sallitaan ainoastaan henkilöille, joilla on tiedonsaantitarve, joista on tehty turvallisuusselvitys kansallisten säädösten ja määräysten mukaisesti ja joille on sallittu pääsy tällaiseen tietoon sekä selvitetty heidän vastuunsa turvallisuusluokitellun tiedon suojaamisesta.

Artiklan 4 kohdan mukaan henkilöturvallisuusselvitystä ei edellytetä turvallisuusluokkaan KÄYTTÖ RAJOITETTU / BEGRÄNSAD TILLGÅNG tai “EINGESCHRÄNKT” kuuluvaan turvallisuusluokiteltuun tietoon pääsemiseksi.

Artiklan 5 kohdan mukaan turvallisuusluokiteltua tietoa saa käyttää ainoastaan siihen tarkoitukseen, jota varten se on luovutettu. Velvoitetta vastaava säännös on kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 6 §:n 2 momentissa.

Artiklan 6 kohdan mukaan kumpikin osapuoli tunnustaa toisen osapuolen antamat todistukset turvallisuusselvityksistä tämän sopimuksen soveltamisalalla.

Artiklan määräykset ovat sopusoinnussa Suomen voimassaolevan turvallisuusluokitellun tiedon suojaamista koskevan lainsäädännön kanssa.

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 toimivaltaiselle turvallisuusviranomaiselle, onko ehdotetulle hankeosapuolelle, joka osallistuu turvallisuusluokiteltua sopimusta edeltäviin neuvotteluihin tai tällaisen sopimuksen täytäntöönpanoon, annettu vaadittua turvallisuusluokkaa vastaava asianmukainen todistus turvallisuusselvityksestä. Jollei hankeosapuolella ole tällaista todistusta, luovuttavan osapuolen toimivaltainen turvallisuusviranomainen voi pyytää vastaanottajan toimivaltaista turvallisuusviranomaista tekemään hankeosapuolta koskevan turvallisuusselvityksen.

Artiklan 2 kohdan mukaan avoimen tarjouskilpailun tapauksessa vastaanottavan osapuolen toimivaltainen turvallisuusviranomainen voi antaa luovuttavan osapuolen toimivaltaiselle turvallisuusviranomaiselle asianmukaiset todistukset turvallisuusselvityksistä ilman virallista pyyntöä.

Artiklan 3 kohdan mukaan yritysturvallisuusselvitystä ei edellytetä turvallisuusluokkaan KÄYTTÖ RAJOITETTU / BEGRÄNSAD TILLGÅNG tai "EINGESCHRÄNKT" kuuluvaa turvallisuusluokiteltua sopimusta varten.

Artiklan 4 kohdan mukaan jotta turvallisuutta voidaan valvoa ja ohjata riittävästi, turvallisuusluokitellussa sopimuksessa on oltava asianmukaiset tämän sopimuksen liitteessä 1 tarkoitetut turvallisuusmääräykset, mukaan lukien luokitusohjeet. Luovuttavan osapuolen toimivaltainen turvallisuusviranomainen toimittaa kopion turvallisuusmääräyksistä vastaanottajan toimivaltaiselle turvallisuusviranomaiselle.

Artiklan 5 kohdan mukaan alihankkijoihin sovelletaan samoja turvallisuusvaatimuksia, mukaan lukien asianmukaiset selvitykset, kuin turvallisuusluokitellun sopimuksen tehneeseen hankeosapuoleen.

Turvallisuusluokiteltuja sopimuksia koskevat kansalliset säännökset sisältyvät kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 1 § 2 momenttiin (soveltaminen elinkeinonharjoittajaan), 2 §:n 2 kohtaan (erityissuojattava tietoaineisto), 2 §:n 3 kohtaan (turvallisuusluokiteltu sopimus), 6 §:ään (salassapitovelvollisuus ja tietojen käyttö), 7 §:ään (vaitiolovelvollisuus ja hyväksikäyttökielto), 10 §:ään (tiloihin liittyvät turvallisuusvaatimukset), 12 §:ään (yritysturvallisuusselvitystodistus, sen voimassaolo ja peruuttaminen), 14 §:ään (todistusta koskevien tietojen merkitseminen turvallisuusselvitysrekisteriin), 16 §:ään (tiedonantovelvollisuus) sekä 18 §:n 2 momenttiin (kansainvälisen toimielimen ja sopimusvaltion edustajien vierailut). Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 18 §:n 2 momentissa säädetään yrityksen velvollisuudesta sallia viranomaisen ja kansainvälisen toimielimen tai sopimusvaltion edustajan tutustuminen turvallisuusjärjestelyihinsä ja toimitiloihinsa, milloin se on tarpeen kansainvälisen tietoturvallisuusvelvoitteen toteuttamiseksi. Turvallisuusselvityslain 40 §:ssä säädetään yrityksen toimivaltaiselle viranomaiselle antamasta sitoumuksesta tietoturvallisuustason säilyttämiseksi sekä viranomaisen pääsemiseksi yrityksen tiloihin tietoturvallisuustason säilyttämisen valvomiseksi. Artiklan mukaiset sopimusvelvoitteet vastaavat kansallisen sääntelyn vaatimuksia.

7 artikla. *Turvallisuusluokitellun tiedon välittäminen.* Artikla sisältää määräykset siitä, miten osapuolet välittävät toisilleen turvallisuusluokiteltua tietoa ei-sähköisessä sekä sähköisessä muodossa.

Artiklan 1 kohdan mukaan osapuolet välittävät turvallisuusluokitellun tiedon toisilleen käyttäen suojattuja hallitusten välisiä kanavia tai muutoin siten kuin niiden toimivaltaiset turvallisuusviranomaiset keskenään sopivat. Turvallisuusluokkaan LUOTTAMUKSELLI-

NEN/KONFIDENTIELL tai ”VERTRAULICH” tai sitä ylempään turvallisuusluokkaan merkityn tiedon vastaanottaminen vahvistetaan kirjallisesti.

Artiklan 2 kohdan mukaan turvallisuusluokiteltua tietoa välitetään osapuolten välillä sähköisesti ainoastaan toimivaltaisten turvallisuusviranomaisten keskenään sopimilla turvallisilla keinoilla.

Artiklan määräykset ovat sopusoinnussa tietoturvallisuusasetuksen asiakirjan välittämistä koskevan 18 §:n ja asiakirjan siirtämistä tietoverkossa koskevan 19 §:n kanssa.

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

Artiklan 1 kohdan mukaan kaikkiin turvallisuusluokitellun tiedon kopioihin ja käännöksiin tehdään asianmukaiset turvallisuusluokitusmerkinnät, ja ne suojataan kuten alkuperäinen turvallisuusluokiteltu tieto. Saman kohdan mukaan käännöksiä tehdään ja kopioita otetaan ainoastaan viralliseen tarkoitukseen tarvittava vähimmäismäärä.

Artiklan 2 kohdan mukaan kaikkiin käännöksiin tehdään asianmukainen käännöskielinen merkintä siitä, että käännökset sisältävät luovuttavan osapuolen turvallisuusluokiteltua tietoa.

Artiklan 3 kohdan mukaan turvallisuusluokkaan ERITTÄIN SALAINEN / YTTERST HEMLIG tai “STRENG GEHEIM” merkittyä tietoa saa kääntää tai kopioida ainoastaan luovuttavan osapuolen kirjallisella suostumuksella.

Artiklan 4 kohdan mukaan turvallisuusluokkaan ERITTÄIN SALAINEN / YTTERST HEMLIG tai “STRENG GEHEIM” merkittyä tietoa ei saa hävittää ilman luovuttavan osapuolen kirjallista ennakkosuostumusta. Tieto palautetaan saman kohdan mukaan luovuttavalle osapuolelle sen jälkeen, kun osapuolet katsovat, ettei sitä enää tarvita.

Artiklan 5 kohdan mukaan turvallisuusluokkaan SALAINEN/HEMLIG tai “GEHEIM” tai alempaan 4 artiklan mukaiseen turvallisuusluokkaan merkitty tieto hävitetään sen jälkeen, kun vastaanottaja katsoo, ettei sitä enää tarvita, vastaanottajan kansallisten säädösten ja määräysten mukaisesti.

Artiklan 6 kohdan mukaan jos kriisitilanne estää sopimuksen mukaisesti luovutetun turvallisuusluokitellun tiedon suojaamisen, tieto hävitetään välittömästi. Vastaanottava osapuoli ilmoittaa turvallisuusluokitellun tiedon tämän kohdan mukaisesta hävittämisestä luovuttavan osapuolen toimivaltaiselle turvallisuusviranomaiselle mahdollisimman pian.

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 sekä 21 §:ssä säädetään asiakirjan arkistoimisesta ja hävittämisestä.

9 artikla. *Vierailut.*

Artiklan 1 kohdan mukaan vierailuihin, joihin liittyy pääsy turvallisuusluokkaan LUOTTAMUKSELLINEN/KONFIDENTIELL tai “VERTRAULICH” tai sitä ylempään turvallisuusluokkaan kuuluvaan tietoon, vaaditaan isäntäosapuolen toimivaltaisen turvallisuusviranomaisen kirjallinen ennakkolupa. Saman kohdan 1 a) – b) alakohtien mukaan vierailijoille sallitaan

pääsy tietoon ainoastaan, jos vieraat lähettävän osapuolen toimivaltainen turvallisuusviranomainen on antanut heille luvan pyydettyyn yhteen tai useampaan vierailuun sekä mikäli heille on annettu asianmukainen todistus henkilöturvallisuusselvityksestä.

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

Artiklan 3 kohdan mukaan toistuvia vierailuja koskevat luvat ovat voimassa enintään 12 kuukautta.

10 artikla. *Turvallisuusyhteistyö.* Artiklassa on määräys kansallisten turvallisuusviranomaisten ja toimivaltaisten turvallisuusviranomaisten välisestä turvallisuusyhteistyöstä.

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

Artiklan 2 kohdan mukaan varmistaakseen läheisen yhteistyön sopimuksen täytäntöönpanossa toimivaltaiset turvallisuusviranomaiset neuvottelevat keskenään sekä antavat toisilleen tietoa turvallisuusluokitellun tiedon suojaamista koskevista kansallisista turvallisuusnormeistaan, menettelyistään ja käytännöistään, sekä näiden merkittävistä muutoksista. 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 voivat myös vierailla toistensa luona keskustellakseen sellaisten toimien täytäntöönpanosta, jotka hankeosapuoli toteuttaa turvallisuusluokiteltuun sopimukseen liittyvän turvallisuusluokitellun tiedon suojaamiseksi.

Artiklan 4 kohdan mukaan turvallisuusviranomaiset avustavat pyynnöstä toisiaan turvallisuusselvityksiin liittyvissä menettelyissä kansallisten säädösten ja määräystensä mukaisesti. Turvallisuusselvityslain 26 §:n 2 momentin 1 kohdan mukaan turvallisuusselvitystä laativa toimivaltainen viranomainen voi viran puolesta kansainvälisen sopimuksen tai säädöksen mukaisesti hankkia ulkomaan viranomaiselta turvallisuusselvityslain 25 §:n 1 momentin 1-3 kohdissa ja tietyin edellytyksin 4 kohdassa tarkoitettuja tietoja vastaavan selvityksen. Kohdan mukainen sopimusvelvoite vastaa kansallisen sääntelyn vaatimuksia.

Artiklan 5 kohdan mukaan kansalliset turvallisuusviranomaiset ilmoittavat viipymättä toisilleen asianomaisten turvallisuusselvityksistä annettujen todistusten muutoksista.

11 artikla. *Tietoturvaloukkaus.* Artiklan 1 kohdan mukaan kumpikin osapuoli ilmoittaa viipymättä kirjallisesti toiselle osapuolelle epäillystä tai todetusta tietoturvaloukkauksesta, joka kohdistuu sopimuksen soveltamisalaan kuuluvaan turvallisuusluokiteltuun tietoon.

Artiklan 2 kohdan mukaan se osapuoli, jonka lainkäyttövaltaan asia kuuluu, tutkii epäillyn tai todetun tietoturvaloukkauksen viipymättä. Toinen osapuoli tekee tarvittaessa tutkintayhteistyötä.

Artiklan 3 kohdan mukaan se osapuoli, jonka lainkäyttövaltaan asia kuuluu, toteuttaa kansallisten säädöstensä ja määräystensä mukaisesti kaikki mahdolliset asianmukaiset toimet rajoittaakseen artiklan 1 kohdassa tarkoitettujen tietoturvaloukkausten seurauksia ja estääkseen tietoturvaloukkausten jatkumisen. Toiselle osapuolelle ilmoitetaan 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 kustannuksistaan, jotka niille aiheutuvat sopimuksesta johtuvien velvoitteiden täyttämisestä.

13 artikla. *Riitojen ratkaiseminen*. Artiklan mukaan kaikki osapuolten väliset riidat, jotka koskevat sopimuksen tulkintaa tai soveltamista, ratkaistaan yksinomaan osapuolten välisin neuvotteluin.

14 artikla. *Loppumääräykset*. Artiklassa on sopimuksen voimaantuloa, muuttamista, irtisanomista sekä irtisanomisesta johtuvia velvollisuuksia koskevat määräykset.

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

Artiklan 2 kohdan mukaan 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.

Artiklan 3 kohdan mukaan osapuoli voi irtisanoa sopimuksen ilmoittamalla asiasta kirjallisesti toiselle osapuolelle diplomaattiteitse kuuden 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.

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 Itävallan 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 säädettäisiin valtioneuvoston asetuksella.

3§. Lain voimaantulosta säädettäisiin valtioneuvoston asetuksella. Laki on tarkoitettu tulemaan voimaan samanaikaisesti kuin sopimus saatetaan Suomen osalta voimaan.

3 Voimaantulo

Suomen ja Itävallan välisen sopimuksen 14 artiklan 1 kohdan mukaan osapuolet ilmoittavat toisilleen, kun sopimuksen voimaantulon edellyttämät kansalliset toimet on toteutettu. Sopimus tulee saman kohdan mukaan 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.

Sopimus ei sisällä Ahvenanmaan maakunnan toimivaltaan kuuluvia määräyksiä, eikä siten edellytä maakunnan suostumusta Ahvenanmaan itsehallintolain (1144/1991) 59 §:n mukaisesti.

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 muun muassa turvallisuusluokitellulla tiedolla, turvallisuusluokitellulla sopimuksella, 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 ulkoasiainministeriön alaisuudessa toimiva kansallinen turvallisuusviranomainen (NSA). Sopimusmääräys vastaa kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 4 §:n 1 momenttia. Määräys on siten toteava, eikä sen siten ole katsottu 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 tietoturvallisuusvelvoitteista 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 tietoturvallisuusvaatimuksia 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 artiklan 2 kohdassa on kyse sopimuksen ydinmääräyksestä, jonka mukaan osapuolet eivät salli kolmansille osapuolille pääsyä turvallisuusluokiteltuun tietoon ilman luovuttavan osapuolen kirjallista ennakkosuostumusta, ja 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 ja tallenteesta. 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. Sopimuksen 5 artiklan 3 kohdassa määrätään myös osapuolten velvollisuudesta teettää asianmukainen turvallisuusselvitys henkilöistä, joille sallitaan pääsy kohdassa 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 turvallisuusselvityslaissa. Määräys kuuluu siten lainsäädännön alaan ja edellyttää eduskunnan suostumusta voimaan tullakseen. Sopimuksen 5 artiklan 5 kohdan mukaan turvallisuusluokiteltua tietoa saa käyttää ainoastaan siihen tarkoitukseen, jota varten se on luovutettu. Velvoitetta vastaava säännös on kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 6 §:n 2 momentissa. Artiklan määräykset kuuluvat näin ollen lainsäädännön alaan.

Sopimuksen 6 artiklassa on määräykset turvallisuusluokitelluista sopimuksista ja niitä tekevien yritysten turvallisuusselvityksistä. Alihankkijoihin sovelletaan samoja turvallisuusvaatimuksia kuin turvallisuusluokitellun sopimuksen tehneeseen hankeosapuoleen. Kansainvälisessä tietoturvallisuusvelvoitteessa edellytettyä yritysturvallisuusselvitystä ja sen perusteella annettavaa yritysturvallisuusselvitystodistusta, sen voimassaoloa sekä sen peruuttamista koskevat säännökset sisältyvät kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 12 §:ään. Vastaavat säännökset yritysturvallisuusselvityksen laatimisesta sisältyvät turvallisuusselvityslakiin.

Sopimuksen 11 artiklassa edellytetään, että kansalliset turvallisuusviranomaiset ilmoittavat viipymättä toisilleen epäillystä tai todetusta turvallisuusluokiteltuun tietoon kohdistuneesta tietoturvaloukkauksesta. Saman artiklan mukaan sen osapuolen, jonka lainkäyttövaltaan asia kuuluu, tulee tutkia tapahtuma viipymättä. Edelleen saman artiklan mukaan sen osapuolen, jonka lainkäyttövaltaan asia kuuluu, tulee toteuttaa kansallisten säädöstensä ja määräystensä mukaisesti kaikkiin mahdolliset asianmukaiset toimet rajoittaakseen artiklassa tarkoitettujen tietoturvaloukkausten seurauksia ja estääkseen tietoturvaloukkausten jatkumisen. Toiselle osapuolelle tulee ilmoittaa tutkinnan ja toteutettujen toimien tuloksista. 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 kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa. 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 lain 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 Itävallan 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 Itävallan liittohallituksen välillä Wienissä 24 päivänä marraskuuta 2017 tehdyn sopimuksen.*

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

Lakiehdotus

Laki

turvallisuusluokitellun tiedon vastavuoroisesta suojaamisesta Itävallan kanssa tehdystä sopimuksesta

Eduskunnan päätöksen mukaisesti säädetään:

1 §

Turvallisuusluokitellun tiedon vastavuoroisesta suojaamisesta Suomen tasavallan hallituksen ja Itävallan liittohallituksen välillä Wienissä 24 päivänä marraskuuta 2017 tehdyn sopimuksen lainsäädännön alaan kuuluvat määräykset ovat lakina voimassa sellaisina kuin Suomi on niihin sitoutunut.

2 §

Sopimuksen muiden kuin lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta säädetään valtioneuvoston asetuksella.

3 §

Tämän lain voimaantulosta säädetään valtioneuvoston asetuksella.

Helsingissä 25 päivänä tammikuuta 2018

Pääministeri

JUHA SIPILÄ

Ulkoministeri Timo Soini

Sopimusteksti

**SOPIMUS
SUOMEN TASAVALLAN HALLITUKSEN
JA
ITÄVALLAN LIITTOHALLITUKSEN
VÄLILLÄ
TURVALLISUUSLUOKITELLUN
TIEDON VASTAVUOROISESTA
SUOJAAMISESTA**

Suomen tasavallan hallitus ja Itävallan liittohallitus, jäljempänä "osapuolet",

suojatakseen turvallisuusluokiteltua tietoa, joka liittyy erityisesti ulko-, puolustus-, turvallisuus- ja poliisiasioihin sekä tiede- ja yritysasioihin ja teknisiin asioihin ja jota vaihdetaan suoraan osapuolten välillä tai niiden lainkäyttövaltaan kuuluvien turvallisuusluokiteltua tietoa käsittelevien 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 turvallisuusluokiteltu ja johon on tehty luokitusmerkintä jommankumman osapuolen kansallisten säädösten ja määräysten mukaisesti tarkoituksena varmistaa tiedon suojaa-

**AGREEMENT
BETWEEN
THE GOVERNMENT OF THE REPUBLIC
OF FINLAND
AND
THE AUSTRIAN FEDERAL
GOVERNMENT
ON
MUTUAL PROTECTION OF CLASSIFIED INFORMATION**

The Government of the Republic of Finland and the Austrian Federal Government, hereinafter referred to as “the Parties”,

in order to protect Classified Information related especially to foreign affairs, defence, security, police or scientific, industrial and technological matters and exchanged directly between the Parties, or legal entities or individuals that handle 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 generated in the process of co-operation 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 applied and which has been marked in accordance with the national laws and regulations of either Party, in order to ensure protection against a Breach of Security as de-

minen tämän artiklan f alakohdassa määritellyltä tietoturvaloukkaukselta, 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, joka sisältää tai johon liittyy turvallisuusluokiteltua tietoa;

c) *luovuttava osapuoli* tarkoittaa osapuolta, joka luovuttaa turvallisuusluokitellun tiedon tai jonka alaisuudessa turvallisuusluokiteltu tieto tuotetaan;

d) *vastaanottaja* tarkoittaa sitä osapuolta ja sen lainkäyttövaltaan kuuluvaa oikeushenkilöä tai luonnollista henkilöä, jolle luovuttava osapuoli luovuttaa turvallisuusluokitellun tiedon;

e) *toimivaltainen turvallisuusviranomainen* tarkoittaa 3 artiklassa tarkoitettua kansallista turvallisuusviranomaista, määrättyä turvallisuusviranomaista tai muuta toimivaltaista elintä, joka on osapuolten kansallisten säädösten ja määräysten mukaisesti valtuutettu vastaamaan tämän sopimuksen täytäntöönpanosta;

f) *tietoturvaloukkaus* tarkoittaa jommankumman osapuolen kansallisten säädösten ja määräysten vastaista tekoa tai laiminlyöntiä, jonka johdosta turvallisuusluokiteltu tieto saatetaan menettää tai se saattaa vaarantua;

g) *turvallisuusselvitys* tarkoittaa selvitysmenettelyyn perustuvaa myönteistä arviota siitä, voidaanko oikeushenkilölle (yritysturvallisuusselvitys) tai luonnolliselle henkilölle (henkilöturvallisuusselvitys) sallia pääsy tiettyyn turvallisuusluokkaan kuuluvaan turvallisuusluokiteltuun tietoon ja tämän tiedon käsittely kansallisten säädösten ja määräysten mukaisesti;

h) *kolmas osapuoli* tarkoittaa sellaista valtiota, joka ei ole tämän sopimuksen osapuoli, tai sellaista oikeushenkilöä tai luonnollista henkilöä, joka ei kuulu kummankaan osapuolen lainkäyttövaltaan.

fined in paragraph f) of this Article, 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, which contains or involves Classified Information;

c) *Originating Party* means the Party which provides Classified Information or under whose authority Classified Information is generated;

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

e) *Competent Security Authority* means a National Security Authority, a Designated Security Authority or any other competent body authorised in accordance with the national laws and regulations of the Parties, which is responsible for the implementation of this Agreement, as specified in Article 3;

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

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

h) *Third Party* means any State that is not a Party to this Agreement or any legal entity or individual that is not under the jurisdiction of either Party.

3 artikla

Toimivaltaiset turvallisuusviranomaiset

1. Kansalliset turvallisuusviranomaiset (Na-

Article 3

Competent Security Authorities

1. The National Security Authorities

tional Security Authority, NSA), jotka vastaavat yleisesti tämän sopimuksen täytäntöönpanosta, ovat:

(NSAs) responsible for the general implementation of this Agreement are:

Suomen tasavallassa	**Itävallan tasavallassa**
Ulkoasiainministeriö Kansallinen turvallisuusviranomainen (NSA) SUOMI	Federal Chancellery Information Security Commission (NSA) AUSTRIA

In the Republic of Finland:	**In the Republic of Austria**
Ministry for Foreign Affairs National Security Authority (NSA) FINLAND	Federal Chancellery Information Security Commission (NSA) AUSTRIA

2. Osapuolet antavat toisilleen tiedoksi diplomaattiteitse mahdolliset muut toimivaltaiset turvallisuusviranomaiset, jotka vastaavat tämän sopimuksen täytäntöönpanosta, sekä näiden viranomaisten mahdolliset myöhemmät muutokset. Nämä tiedoksiannot sisältävät myös kansallisten turvallisuusviranomaisten ja muiden toimivaltaisten turvallisuusviranomaisten yhteystiedot.

2. The Parties shall notify each other through diplomatic channels of other Competent Security Authorities which are responsible for the implementation of this Agreement, as well as any subsequent changes thereof. Such notifications shall also include contact information on the NSAs and the other Competent Security Authorities.

4 artikla

Turvallisuusluokitukset

1. Tämän sopimuksen mukaisesti luovutettavaan turvallisuusluokiteltuun tietoon merkitään asianomainen 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 in accordance with the national laws and regulations of the Parties.
2. The classification levels shall correspond to one another as follows:

Suomen tasavalta	Itävallan tasavalta	Englanninkielinen vastine
ERITTÄIN SALAINEN tai YTTERST HEMLIG	STRENG GEHEIM	TOP SECRET
SALAINEN tai HEMLIG	GEHEIM	SECRET
LUOTTAMUKSELLINEN tai KONFIDENTIELL	VERTRAULICH	CONFIDENTIAL
KÄYTTÖ RAJOITETTU tai BEGRÄNSAD TILLGÅNG	EINGESCHRÄNKT	RESTRICTED

The Republic of Finland	The Republic of Austria	English translation
ERITTÄIN SALAINEN or YTTERST HEMLIG	STRENG GEHEIM	TOP SECRET
SALAINEN or HEMLIG	GEHEIM	SECRET
LUOTTAMUKSELLINEN or KONFIDENTIELL	VERTRAULICH	CONFIDENTIAL
KÄYTTÖ RAJOITETTU or BEGRÄNSAD TILLGÅNG	EINGESCHRÄNKT	RESTRICTED

3. Vastaanottaja varmistaa, ettei turvallisuusluokituksia muuteta eikä kumota, ellei luovuttava osapuoli anna siihen kirjallista lupaa. Luovuttava osapuoli ilmoittaa viipymättä vastaanottajalle, jos välitetyn turvallisuusluokitellun tiedon turvallisuusluokkaa muutetaan tai se kumotaan.

3. The Recipient shall ensure that classifications are not altered or revoked, except as authorised in writing by the Originating Party. The Originating Party shall inform the Recipient without delay about any alteration or revocation of the security classification level of the transmitted Classified Information.

5 artikla

Article 5

Turvallisuusluokitellun tiedon suojaaminen

1. Osapuolet toteuttavat kaikki asianmukaiset toimet suojatakseen tässä sopimuksessa tarkoitettua turvallisuusluokiteltua tietoa ja mahdollistavat tämän suojaamisen tarvittavan valvonnan. Ne antavat tälle tiedolle vähintään samantasoisen suojan kuin omalle vastaavaan turvallisuusluokkaan kuuluvalle tiedolleen kansallisten säädöstensä ja määräystensä mukaisesti.

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

3. Pääsy turvallisuusluokiteltuun tietoon sallitaan ainoastaan henkilöille, joilla on tiedonsaantitarve, joista on tehty turvallisuusselvitys kansallisten säädösten ja määräysten mukaisesti ja joille on sallittu pääsy tällaiseen tietoon sekä selvitetty heidän vastuunsa turvallisuusluokitellun tiedon suojaamisesta.

4. Henkilöturvallisuusselvitystä ei edellytetä turvallisuusluokkaan KÄYTTÖ RAJOITETTU / BEGRÄNSAD TILLGÅNG tai EINGESCHRÄNKT kuuluvaan turvallisuusluokiteltuun tietoon pääsemiseksi.

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

6. Kumpikin osapuoli tunnustaa toisen osapuolen antamat todistukset turvallisuusselvityksistä tämän sopimuksen soveltamisalalla.

Protection of Classified Information

1. The Parties shall take all appropriate measures to protect Classified Information referred to in this Agreement and shall provide for the necessary control of this protection. They shall afford such information at least the same protection as they afford to their own information at the corresponding classification level in accordance with their national laws and regulations.

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-know and who, in accordance with the 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. A Personnel Security Clearance is not required for access to Classified Information at the KÄYTTÖ RAJOITETTU / BEGRÄNSAD TILLGÅNG or EINGESCHRÄNKT level.

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

6. Within the scope of this Agreement, each Party shall recognize the Security Clearances issued by the other Party.

6 artikla

Turvallisuusluokitellut sopimukset

1. Vastaanottajan toimivaltainen turvallisuusviranomainen ilmoittaa pyynnöstä luovuttavan osapuolen toimivaltaiselle turvallisuusviranomaiselle, onko ehdotetulle hankeosapuolelle, joka osallistuu turvallisuusluokiteltua sopimusta edeltäviin neuvotteluihin tai tällaisen sopimuksen täytäntöönpanoon, annettu vaadittua turvallisuusluokkaa vastaava asianmukainen todistus turvallisuusselvityksestä. Jollei hankeosapuolella ole tällaista todistusta, luovuttavan osapuolen toimivaltainen turvallisuusviranomainen voi pyytää vas-

Article 6

Classified Contracts

1. Upon request, the Competent Security Authority of the Recipient shall inform the Competent Security Authority of the Originating Party whether a proposed contractor participating in precontract negotiations or in the implementation of a Classified Contract has been issued an appropriate Security Clearance corresponding to the required security classification level. If the contractor does not hold such a Security Clearance, the Competent Security Authority of the Originating Party may request that the contractor

taanottajan toimivaltaista turvallisuusviranomaista tekemään hankeosapuolta koskevan turvallisuusselvityksen.

2. Jos on kyse avoimesta tarjouskilpailusta, vastaanottajan toimivaltainen turvallisuusviranomainen voi antaa luovuttavan osapuolen toimivaltaiselle turvallisuusviranomaiselle asianmukaiset todistukset turvallisuusselvityksestä ilman virallista pyyntöä.

3. Yritysturvallisuusselvitystä ei edellytetä turvallisuusluokkaan KÄYTTÖ RAJOITETTU / BEGRÄNSAD TILLGÅNG tai EINGESCHRÄNKT kuuluvaa turvallisuusluokiteltua sopimusta varten.

4. Jotta turvallisuutta voidaan valvoa ja ohjata riittävästi, turvallisuusluokitellussa sopimuksessa on oltava asianmukaiset tämän sopimuksen liitteessä 1 tarkoitetut turvallisuusmääräykset, mukaan lukien luokitusohjeet. Luovuttavan osapuolen toimivaltainen turvallisuusviranomainen toimittaa kopion turvallisuusmääräyksistä vastaanottajan toimivaltaiselle turvallisuusviranomaiselle.

5. Alihankkijoihin sovelletaan samoja turvallisuusvaatimuksia, mukaan lukien asianmukaiset selvitykset, kuin turvallisuusluokitellun sopimuksen tehneeseen hankeosapuoleen.

be security cleared by the Competent Security Authority of the Recipient.

2. In the case of an open tender the Competent Security Authority of the Recipient may provide the Competent Security Authority of the Originating Party with the relevant Security Clearance certificates without a formal request.

3 A Facility Security Clearance is not required for Classified Contracts at KÄYTTÖ RAJOITETTU / BEGRÄNSAD TILLGÅNG or EINGESCHRÄNKT level.

4. To allow adequate security supervision and control, a Classified Contract shall contain appropriate security provisions as specified in Annex 1, including a security classification guide. A copy of the security provisions shall be forwarded by the Competent Security Authority of the Originating Party to the Competent Security Authority of the Recipient.

5. Sub-contractors shall be subject to the same security requirements, including due certifications, as the contractor which concluded the Classified Contract.

7 artikla

Turvallisuusluokitellun tiedon välittäminen

1. Osapuolet välittävät turvallisuusluokitellun tiedon toisilleen käyttäen suojattuja hallitusten välisiä kanavia tai muutoin siten kuin niiden toimivaltaiset turvallisuusviranomaiset keskenään sopivat. Turvallisuusluokkaan LUOTTAMUKSELLINEN/KONFIDENTIELL tai VERTRAULICH tai sitä ylempään turvallisuusluokkaan merkityn tiedon vastaanottaminen vahvistetaan kirjallisesti.

2. Turvallisuusluokiteltua tietoa välitetään osapuolten välillä sähköisesti ainoastaan toimivaltaisten turvallisuusviranomaisten keskenään sopimilla turvallisilla keinoilla.

Article 7

Transmission of Classified Information

1. Classified Information shall be transmitted between the Parties through secured government-to-government channels or as otherwise agreed between their Competent Security Authorities. Receipt of Classified Information marked LUOTTAMUKSELLINEN/KONFIDENTIELL or VERTRAULICH and above shall be acknowledged in writing.

2. Classified Information shall be transmitted between the Parties electronically only by secure means agreed between the Competent Security Authorities.

8 artikla

Turvallisuusluokitellun tiedon kääntäminen, kopiointi ja hävittäminen

Article 8

Translation, reproduction and destruction of Classified Information

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 ERITTÄIN SALAINEN / YTTERST HEMLIG tai STRENG GEHEIM merkittyä tietoa saa kääntää tai kopioida ainoastaan luovuttavan osapuolen kirjallisella suostumuksella.

4. Turvallisuusluokkaan ERITTÄIN SALAINEN / YTTERST HEMLIG tai STRENG GEHEIM merkittyä tietoa ei saa hävittää ilman luovuttavan osapuolen kirjallista ennakkosuostumusta. Tieto palautetaan luovuttavalle osapuolelle sen jälkeen, kun osapuolet katsovat, ettei sitä enää tarvita.

5. Turvallisuusluokkaan SALAINEN/HEMLIG tai GEHEIM tai alempaan 4 artiklan mukaiseen turvallisuusluokkaan merkitty tieto hävitetään sen jälkeen, kun vastaanottaja katsoo, ettei sitä enää tarvita, vastaanottajan kansallisten säädösten ja määräysten mukaisesti.

6. Jos kriisitilanne estää tämän sopimuksen mukaisesti luovutetun turvallisuusluokitellun tiedon suojaamisen, tieto hävitetään välittömästi. Vastaanottaja ilmoittaa turvallisuusluokitellun tiedon hävittämisestä luovuttavan osapuolen toimivaltaiselle turvallisuusviranomaiselle mahdollisimman pian.

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 ERITTÄIN SALAINEN / YTTERST HEMLIG or STRENG GEHEIM shall be translated or reproduced only upon the written consent of the Originating Party.

4. Classified Information marked ERITTÄIN SALAINEN / YTTERST HEMLIG or STRENG GEHEIM 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 SALAINEN/HEMLIG or GEHEIM or with a lower classification level under Article 4, shall be destroyed after it is no longer considered necessary by the Recipient, in accordance with its national laws and regulations.

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

9 artikla

Vierailut

1. Vierailuihin, joihin liittyy pääsy turvallisuusluokkaan LUOTTAMUKSELLINEN/KONFIDENTIELL tai VERTRAULICH tai sitä ylempään turvallisuusluokkaan kuuluvaan tietoon, vaaditaan isäntäosapuolen toimivaltaisen turvallisuusviranomaisen kirjallinen ennakkolupa. Vierailijoille sallitaan pääsy turvallisuusluokiteltuun tie-

Article 9

Visits

1. Visits entailing access to Classified Information at LUOTTAMUKSELLINEN/KONFIDENTIELL or VERTRAULICH or above require prior written permission from the Competent Security Authority of the host Party. Visitors shall only be allowed access where they have been:

toon ainoastaan, jos

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

b) heille on annettu asianmukainen todistus henkilöturvallisuusselvityksestä.

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 12 kuukautta.

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

b) granted an appropriate Personnel Security Clearance.

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 specified in Annex 2 to this Agreement.

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

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

3. Toimivaltaiset turvallisuusviranomaiset voivat myös vierailla toistensa luona keskustellakseen sellaisten toimien täytäntöönpanosta, jotka hankeosapuoli toteuttaa turvallisuusluokiteltuun sopimukseen liittyvän turvallisuusluokitellun tiedon suojaamiseksi.

4. Toimivaltaiset turvallisuusviranomaiset

Article 10

Security co-operation

1. 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 Competent Security Authorities shall consult each other. They shall provide each other with information about their national security standards, procedures and practices for the protection of Classified Information and any substantial changes thereof. To this aim the Competent Security Authorities may visit each other.

3. The Competent Security Authorities may also visit each other in order to discuss the implementation of the measures adopted by a contractor for the protection of Classified Information involved in a Classified Contract.

4. On request, Competent Security Authori-

avustavat pyynnöstä toisiaan kansallisten säädösten ja määräysten mukaisesti turvallisuusselvitysten tekemisessä.

5. Kansalliset turvallisuusviranomaiset ilmoittavat viipymättä toisilleen tämän sopimuksen soveltamisalaan kuuluvien turvallisuusselvityksistä annettujen todistusten muutoksista.

ties shall, in accordance with the national laws and regulations, assist each other in carrying out Security Clearance procedures.

5. The National Security Authorities shall promptly inform each other about changes of Security Clearance certificates falling under this Agreement.

11 artikla

Tietoturvaloukkaus

1. Kumpikin osapuoli ilmoittaa viipymättä kirjallisesti toiselle osapuolelle epäillystä tai todetusta tietoturvaloukkauksesta, joka kohdistuu tämän sopimuksen soveltamisalaan kuuluvaan turvallisuusluokiteltuun tietoon.

2. Se osapuoli, jonka lainkäyttövaltaan asia kuuluu, tutkii epäillyn tai todetun tietoturvaloukkauksen viipymättä. Toinen osapuoli tekee tarvittaessa tutkintayhteistyötä.

3. Se osapuoli, jonka lainkäyttövaltaan asia kuuluu, toteuttaa kansallisten säädöstensä ja määräystensä mukaisesti kaikki mahdolliset asianmukaiset 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 in writing of any suspected or discovered Breach of Security of Classified Information falling under this Agreement.

2. The Party with jurisdiction shall investigate suspected or discovered Breach of Security without delay. The other Party shall, if required, co-operate in the investigation.

3. The Party with jurisdiction shall undertake all possible appropriate measures in accordance with 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 sopimuksesta johtuvien velvoitteiden täyttämisestä.

Article 12

Costs

Each Party shall bear its own costs incurred in the course of implementing its obligations under this Agreement.

13 artikla

Riitojen ratkaiseminen

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

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.

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 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.

Tämän vakuudeksi asianmukaisesti valtuutetut osapuolten edustajat ovat allekirjoittaneet tämän sopimuksen

Wienissä 24. päivänä marraskuuta 2017

kahtena suomen-, saksan- ja englanninkielisenä alkuperäiskappaleena, jonka kaikki tekstit ovat yhtä todistusvoimaiset. Jos syntyy tulkintaeroja, englanninkielinen teksti on ratkaiseva.

SUOMEN TASAVALLAN
HALLITUKSEN PUOLESTA

Anu Laamanen

ITÄVALLAN LIITTOHALLITUKSEN

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.

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

in Vienna on the 24th day of November, 2017

in two originals, in the Finnish, German and English languages, each text being equally authentic. In case of any divergence of interpretation, the English text shall prevail.

FOR THE GOVERNMENT OF THE
REPUBLIC OF FINLAND

Anu Laamanen

FOR THE AUSTRIAN

PUOLESTA	FEDERAL GOVERNMENT
Helmut Tichy	Helmut Tichy

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 therefor;
9. requirements for the period of protecting Classified Information;
10. procedure for destroying or returning Classified Information.

Liite 2

Vierailupyyntö

Tämän sopimuksen 9 artiklassa tarkoitetut vierailupyynnöt on laadittava englannin kielellä, ja niiden on sisällettävä seuraavat tiedot:

1. vierailijan suku- ja etunimi, syntymäpaikka ja -aika ja kansalaisuus; 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, muut yhteystiedot ja yhteyshenkilö sekä muut vierailun tai vierailujen perusteltavuuden määrittämiseksi tarpeelliset tiedot;

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

Annex 2

Request for visit

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

1. the visitor's family name, first name, place and date of birth and nationality, the visitor’s position, with a specification of the employer which the visitor represents, a specification of the project in which the visitor participates, 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, other contact information and point of contact of the establishment or facility to be visited, and any other information useful for determining the justification for the visit or visits;

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