

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

ESITYKSEN PÄÄASIALLINEN SISÄLTÖ

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

Sopimuksen tarkoituksena on varmistaa salassa pidettävän tiedon välittäminen ja suojaaminen Suomen ja Slovenian välillä ulko-, puolustus-, turvallisuus- ja poliisiasioissa sekä teollisuus- tai teknologia-asioissa. Kysymys on arkaluonteisista tietoaineistoista, jotka lähetävässä sopimusvaltiossa on erikseen

luokiteltu korkean tietoturvallisuuden tason toteuttamista edellyttäviksi.

Sopimus tulee voimaan toiseksi seuraavan kuukauden ensimmäisenä päivänä sen jälkeen, kun jälkimmäinen ilmoitus siitä, että sopimuksen voimaansaattamiseksi tarvittavat kansalliset toimenpiteet on saatettu loppuun, on otettu vastaan. Sopimuksen voimaansaatamlaki on tarkoitettu tulemaan voimaan tasavallan presidentin asetuksella säädettävänä ajankohtana samaan aikaan kuin sopimus tulee Suomen osalta voimaan.

SISÄLLYS

ESITYKSEN PÄÄASIALLINEN SISÄLTÖ.....	1
SISÄLLYS.....	2
YLEISPERUSTELUT.....	3
1 JOHDANTO.....	3
2 NYKYTILA.....	4
2.1 Laki kansainvälisistä tietoturvaluokitusvelvoitteista.....	4
Lain yleinen soveltamisala.....	4
Lain suhde julkisuuslainsäädäntöön.....	4
Lain soveltaminen elinkeinonharjoittajiin.....	4
Lain täytäntöönpanoviranomaiset.....	5
Tietojen salassapito ja käytön sääntely.....	5
Turvallisuusluokittelu ja -toimenpiteet.....	6
Henkilöturvallisuus.....	6
Yhteisöturvallisuus selvitys.....	6
2.2 Turvallisuukselvityksiä koskeva lainsäädäntö.....	7
3 ESITYKSEN TAVOITTEET.....	7
4 ESITYKSEN VAIKUTUKSET.....	7
4.1 Vaikutukset kansalaisiin.....	7
4.2 Vaikutukset elinkeinoelämään.....	8
4.3 Taloudelliset vaikutukset.....	8
4.4 Vaikutukset hallintoon.....	8
5 ASIAN VALMISTELU.....	8
YKSITYISKOHTAISET PERUSTELUT.....	9
1 SOPIMUKSEN SISÄLTÖ JA SUHDE SUOMEN LAINSÄÄDÄNTÖÖN.....	9
2 LAKIEHDOTUKSEN PERUSTELUT.....	13
3 VOIMAANTULO.....	13
4 EDUSKUNNAN SUOSTUMUKSEN TARPEELLISUUS JA KÄSITTELYJÄRJESTYS.....	13
4.1 Eduskunnan suostumuksen tarpeellisuus.....	13
4.2 Käsitteilyjärjestys.....	15
LAKIEHDOTUS.....	16
Slovenian kanssa turvallisuusluokitellun tiedon vaihtamisesta ja vastavuoroisesta suojaamisesta tehdyn sopimuksen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta.....	16
SOPIMUSTEKSTI.....	17

YLEISPERUSTELUT

1 Johdanto

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

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

Kansainvälinen tietoturvallisuusyhteistyö, johon Suomikin osallistuu, käsittää perinteisesti diplomaattiseen toimintaan samoin kuin puolustus- ja poliisihallintojen väliseen yhteistyöhön liittyvän ei-julkisen tiedonvaihdon suojaamisen. Välttömän valtiovastuun piiriin kuuluvien kysymysten lisäksi kansainvälisillä tietoturvallisuusvelvoitteilla on kuitenkin kasvava merkitys myös taloudellisen, teollisen ja teknologisen yhteistyön kannalta, joiden puitteissa yhä useammat yritystason hankkeet edellyttävät turvallisuussuojatun 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 sektori on laajenemassa.

Pyrkimyksistä huolimatta ei kuitenkaan ole osoittautunut mahdolliseksi toteuttaa tieto-

turvallisuusalan monenkeskistä yleissopimusta. Pääasiallinen syy tähän ovat kansallisten lainsäädäntöjen ja hallintorakenteiden ja -tapojen eroavaisuudet, jotka puolestaan heijastelevat tietoturvallisuuden sensitiivisyyttä osana kansallista kokonaisturvallisuutta.

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

Tietoturvallisuustarpeiden painottumista enenevässä määrin myös taloudelliseen toimintaan ilmentää Suomen ja Euroopan Avaruusjärjestön (ESA) välinen yhteistyösopimus, jäljempänä ESA:n tietoturvallisuussopimus, niin ikään vuodelta 2004 (SopS 94-95/2004). Sopimuksen eräs keskeinen tavoite on turvata Suomen elinkeinoelämän mahdollisuudet osallistua tasavertaisesti muiden jäsenmaiden kanssa ESA:n turvallisuusluokiteltuihin tarjouskilpailuihin.

Mainittujen sopimusten lisäksi Suomi on tehnyt voimassa olevan tietoturvasopimuksen Slovakian (SopS 116-117/2007), Viron (SopS 12-13/2008), Italian (SopS 23-24/2008), Latvian (SopS 33-34/2008) ja Puolan (SopS 46-47/2008) kanssa. Kuluvana vuonna Suomi on Slovenian kanssa tehdyn sopimuksen lisäksi allekirjoittanut tietoturvallisuussopimuksen Bulgarian (16.4.2008) ja Tšekin (22.5.2008) kanssa. Parafointivaiheeseen ovat edenneet sopimukset Espanjan, Liettuan ja Alankomaiden kanssa. Vireillä on lisäksi hanke EU:n jäsenmaiden välisestä turvallisuusluokitellun tiedon suojaamista koskevasta sopimuksesta.

Suomen ja Slovenian välinen sopimus allekirjoitettiin Ljubljanassa 6 päivänä toukokuuta 2008. Sopimus on neuvoteltu pitkälti

Suomen neuvottelujen pohjaksi esittämän mallisopimuksen perusteella.

2 Nykytila

2.1 Laki kansainvälisistä tietoturvallisuusvelvoitteista

Lain yleinen soveltamisala

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

Lakia kansainvälisistä tietoturvallisuusvelvoitteista sovelletaan erityissuojattaviin tietoineistoihin. Näillä tarkoitetaan salassa pidettäviä asiakirjoja ja materiaaleja, jotka on toimitettu Suomen viranomaiselle ja joiden lähettäjä on kansainvälisen, Suomea sitovan sopimuksen tai muun kansainvälisen velvoitteen mukaisesti tehnyt niihin turvallisuusluokkaa koskevan merkinnän. Omistusoikeus 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 tietoineistoja ovat lisäksi Suomen viranomaisen tai lain soveltamisalan piiriin kuuluvan elinkeinonharjoittajan laatimat asiakirjat, joista ilmenee Suomeen toimitettuihin asiakirjoihin sisältyviä tai materiaalista saatavissa olevia tietoja. Lain soveltamisalan piiriin kuuluvat niin ikään asiakirjat ja materiaalit, jotka on Suomessa tuotettu salassa pidettävän turvallisuusluokitellun tiedon perusteella.

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

Lain suhde julkisuuslainsäädäntöön

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

Lain soveltaminen elinkeinonharjoittajiin

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

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 tarkoitettulla tavalla Suomessa kotipaikkaansa pitävän elinkeinonharjoittajan kanssa, jos tar-

jouskilpailuun osallistuminen tai sopimuksen toteuttaminen voi edellyttää pääsyä erityissuojattavaan tietoaaineistoon (2 § 3 k.).

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

Elinkeinonharjoittajalla ja tämän palveluksessa tai toimeksiannosta toimivalla on erityissuojattavia tietoaaineistoja koskeva salassapitovelvollisuus (6 ja 7 §). Elinkeinonharjoittajalla on myös velvollisuus kansainvälisten tietoturvallisuusvelvoitteiden toteuttamiseksi antaa tietoja sekä sallia viranomaisen ja kansainvälisen toimielimen tai sopimusvaltion edustajan tutustuminen turvallisuusjärjestelyihinsä ja toimitiloihinsa (16 § 2 mom., 18 § 2 mom.).

Lain täytäntöönpanoviranomaiset

Laissa on säännökset niistä viranomaisista, jotka huolehtivat kansainvälisten tietoturvallisuusvelvoitteiden hoitamisesta. Kansallisen turvallisuusviranomaisena (National Security Authority, NSA) kansainvälisten tietoturvallisuusvelvoitteiden toteuttamiseen liittyvissä tehtävissä toimii ulkoasiainministeriö. Puolustusministeriö, pääesikunta ja suojelupoliisi toimivat määrättyinä turvallisuusviranomaisina (Designated Security Authority, DSA). Näille viranomaisille voi kuulua muun ohella tarjous- ja hankintamenettelyihin liittyvien asiakirjojen turvallisuusluokittelu. Henkilöturvallisuuteen liittyvien turvallisuusselvitysten laadinnasta huolehtivat suojelupoliisi ja pääesikunta. Yhteisöturvallisuusselvityksen laadinta kuuluu sen sijaan kaikilta osin pääesikunnalle.

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

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

Tietojen salassapito ja käytön sääntely

Erityissuojattava tietoaaineisto on pidettävä salassa (6 § 1 mom.). Salassapitovelvollisuus koskee myös elinkeinonharjoittajaa tämän ollessaan hankeosapuolena turvallisuusluokitellussa sopimuksissa.

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

Turvallisuusluokittelu ja -toimenpiteet

Laissa säädetään velvollisuudesta merkitä erityissuojattavaan tietoaaineistoon sen turvallisuusluokka. Tietoaaineistoon tehty merkintä turvallisuusluokasta osoittaa, minkälaisia toimenpiteitä on toteutettava aineistoa käsiteltäessä. Mitä korkeampaan turvallisuusluokkaan aineisto kuuluu, sitä tiukempia tietoturvallisuustoimenpiteitä edellytetään. Laissa on yleinen velvoite toteuttaa tietoaaineiston käsittelyssä sen turvallisuusluokkaa koskevia käsittelymääräyksiä sekä valtuus säätää erityissuojattavan tietoaaineiston käsittelyssä noudatettavista turvallisuusluokitusta vastaavista teknisistä turvallisuustoimenpiteistä valtioneuvoston asetuksella.

Turvallisuusluokiteltuja aineistoja käsiteltäessä on lain mukaan huolehdittava siitä, että tietoja säilytetään asianmukaisissa tiloissa. Myös tilojen turvallisuusvaatimuksista voidaan säätää asetuksella (10 §).

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

Henkilöturvallisuus

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

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

tietoturvallisuusvelvoitteen toteuttamiseksi (11 § 1 mom.). Toinen erityissäännös koskee viranomaisten toimivaltaa. Turvallisuus selvityksen tekee pääesikunta silloin kun turvallisuus selvityksen laatiminen on tarpeen puolustushallintoa tai puolustushankintoja koskevan kansainvälisen velvoitteen toteuttamiseksi. Muissa tapauksissa henkilöön liittyvien turvallisuus selvitysten laadinnasta huolehtii suojelupoliisi (11 § 2 mom.). Säännös on turvallisuus selvityksistä annettua lakia täsmällisempi ja siinä otetaan huomioon, minkälaisesta kansainvälisestä velvoitteesta on kysymys.

Turvallisuus selvityksistä annetun lain 10 §:n 2 momentin mukaan turvallisuus selvitykseen ei saa sisällyttää selvityksen laatineen viranomaisen arviota selvityksen kohteena olevan henkilön luotettavuudesta tai sopivuudesta virkaan tai tehtävään, ellei lain 9 §:ssä tarkoitettu valtiosopimus tai muu kansainvälinen velvoite tätä edellytä. Koska pääsääntönä on, että turvallisuus selvitys ei sisällä arviota henkilön luotettavuudesta, laissa kansainvälisistä tietoturvallisuusvelvoitteista on erikseen mainittu henkilön luotettavuuden arviointi. Tällaisen arvion tekee turvallisuus selvityksen perusteella kansallinen turvallisuusviranomainen tai, jos turvallisuusviranomaisten välillä on niin sovittu, tehtävään määrätty turvallisuusviranomainen.

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

Yhteisöturvallisuus selvitys

Yhteisöturvallisuus selvityksellä varmistetaan elinkeinonharjoittajan toimitilojen ja käsittelykäytäntöjen asianmukaisuus sekä henkilöstön osaaminen. Elinkeinonharjoittajan luotettavuuden arvioinnilla varmistutaan erityisesti siitä, kuinka hyvin tämä pystyy huolehtimaan turvallisuusluokiteltujen tietojen suojaamisesta. Yhteisöturvallisuusmenettely ja siihen perustuva arvio toteutetaan pääosin elinkeinonharjoittajalta itseltään saatujen tietojen perusteella sekä tämän toimitilojen tur-

vallisuuden kartoituksella, ja tarvittavista toimenpiteistä huolehditaan elinkeinonharjoittajan kanssa tehtävän sopimuksen avulla. Selvityksen laatii pääesikunta. Selvitystä laadittaessa on otettava huomioon laissa yksilöidyt seikat, muun muassa se, miten suojataan turvallisuusluokiteltuja tietoja oikeudettomalta ilmitulolta, muuttamiselta ja hävittämiseltä, ja miten estetään asiaton pääsy tiloihin, joissa turvallisuusluokiteltuja tietoja käsitellään tai joissa harjoitetaan turvallisuusluokitellussa sopimuksessa tarkoitettua toimintaa.

Pääesikunta voi tehdä lain soveltamisalan piiriin kuuluvan elinkeinonharjoittajan kanssa sopimuksen, jossa elinkeinonharjoittaja sitoutuu toimenpiteisiin kansainvälisten tietoturvallisuusvelvoitteiden toteuttamiseksi (13 §). Sopimuksessa voidaan yksityiskohtaisemmin määritellä ne toimenpiteet, jotka elinkeinonharjoittaja toteuttaa täyttääkseen kansainvälisistä tietoturvallisuusvelvoitteista johtuvat vaatimukset. Sopimuksessa elinkeinonharjoittaja sitoutuu myös tekemään ne mahdolliset tarkistukset toimintaansa, jotka toiminnan turvallisuuskartoituksessa on havaittu. Turvallisuusselvityksen ja mahdollisen sopimuksen jälkeen pääesikunta voi tehdä arvion elinkeinonharjoittajan luotettavuudesta ja antaa tätä koskevan turvallisuustodistuksen (Facility Security Clearance).

2.2 Turvallisuusselvityksiä koskeva lainsäädäntö

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

Turvallisuusselvitys voidaan tehdä virkaan tai tehtävään hakeutuvasta, tehtävään tai koulutukseen otettavasta taikka virkaa tai tehtävää hoitavasta henkilöstä, ja se voi olla perusmuotoinen, laaja tai suppea. Turvallisuusselvitys tehdään laissa määritellyissä tapauksissa, kuten silloin, kun Suomea sitova valtiosopimus tai muu kansainvälinen velvoite edellyttää turvallisuusselvityksen tekemistä

tai sen perusteella laaditun todistuksen esittämistä.

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

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

3 Esityksen tavoitteet

Esityksen tavoitteena on saattaa voimaan Suomen ja Slovenian välinen tietoturvallisuus sopimus ja sillä tavoin parantaa maiden välistä yhteistyötä sekä turvata suomalaisten yritysten mahdollisuudet osallistua sellaisiin kansainvälisiin sekä Suomen ja Slovenian välisiin hankkeisiin, joiden toteuttaminen saattaa edellyttää arkaluonteisten salassa pidettävien tietojen vaihtoa.

4 Esityksen vaikutukset

4.1 Vaikutukset kansalaisiin

Sopimuksen voimaansaattamisen myötä Sloveniasta Suomeen toimitettuihin turvallisuusluokiteltuihin tietoihin ja materiaaleihin sovellettaisiin lakia kansainvälisistä tietoturvallisuusvelvoitteista. Lakiin sisältyy erityissäännös, jonka mukaan toisen sopimuspuolen salassa pidettävät ja turvallisuusluokitellut asiakirjat ja niihin sisältyvät tiedot ovat myös Suomessa salassa pidettäviä. Säännös poikkeaa muodoltaan julkisuuslain yleistä etua koskevista salassapitosäännöksistä, joissa salassapito on useimmissa tapauksissa riippuvainen siitä, minkälaisia vaikutuksia tietojen antamisella olisi suojattavalle edulle. Kansainvälisistä tietoturvallisuusvelvoitteista an-

netun lain mukainen salassapito on näin ollen sanamuodon mukaan kattavampi kuin yleisessä julkisuuslaissa.

Suomen ja Slovenian välisessä sopimuksessa on kysymys asiakirjoista, joita toinen sopimuspuoli pitää salassa pidettävänä ja jotka se on määritellyt ja merkinnyt korkean tietoturvallisuuden tasoa edellyttäviksi. Tällaisia asiakirjoja on säännönmukaisesti pidettävä salaisina myös julkisuuslain 24 §:n 1 momentin 2 kohdan mukaan. Merkittävimpana erona on se, että viranomaisella ei olisi kansainvälisessä tietoturvallisuusvelvoitteessa tarkoitettuun asiakirjaan kohdistuvaa tiedonsaantipyyntöä ratkaistessaan velvollisuutta erikseen perustella tiedon antamisesta aiheutuvaa vahinkoa. Tiedonsaantipyyntö olisi muutoin käsiteltävä julkisuuslain mukaisesti. Siten viranomaisen on varmistettava, että asiakirjaan merkitty salaisuusluokka vastaa sopimuksessa sovittua. Jos luokituksen oikeellisuudesta tai siitä, minkä asiakirjan tietojen vuoksi luokitusmerkintä on tehty, syntyy epäselvyyttä, viranomaisen on otettava yhteyttä asiakirjan laatineeseen sopimuspuoleen.

Edellä olevan perusteella voidaan arvioida, että Suomen ja Slovenian välisen tietoturvalisuussopimuksen voimaansaattamista koskeva lakiehdotus ei asiallisesti vaikuta kansalaisten tiedonsaantia vähentävästi suhteessa siihen, mitä tiedonsaanti yleisen lainsäädännön mukaan on.

Henkilöturvallisuus on keskeinen tietoturvallisuuden osa-alue. Koska jo laki kansainvälisistä tietoturvalvelvoitteista edellyttää turvallisuus selvityksistä annetun lain mukaisen menettelyn käyttämistä henkilöstön luotettavuuden varmistamisesta, ehdotetun voimaansaattamislain hyväksyminen ei tarkoittaisi sitä, että kansalaisten yksityisyyselämän ja henkilötietojen suojaa kavennettaisiin aikaisempaan verrattuna.

4.2 Vaikutukset elinkeinoelämään

Sopimus antaa suomalaiselle teollisuudelle, toisin kuin tähän asti, mahdollisuudet saada sellaisia tilauksia tai osallistua sellaisiin hankkeisiin, joiden toteuttaminen edellyttää pääsyä Slovenian turvallisuusluokiteltuihin

tietoihin. Vastaavasti sopimus antaa Slovenian teollisuudelle, toisin kuin tähän asti, mahdollisuuden saada sellaisia tilauksia tai osallistua sellaisiin hankkeisiin, joiden toteuttaminen edellyttää pääsyä Suomen turvaluokiteltuun tietoon.

4.3 Taloudelliset vaikutukset

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

Tässä yhteydessä on kuitenkin syytä mainita vireillä oleva kansainvälisistä tietoturvalisuusvelvoitteista annetun lain muutos, jonka perusteella suojelupoliisi ottaisi vastatakseen siviilejä koskevat yhteisöturvallisuus selvitykset mahdollisesti jo vuoden 2009 alusta. Tällä hetkellä kaikista yhteisöturvallisuus selvityksistä vastaa Pääesikunta. Muutoksesta aiheutuvat taloudelliset, hallinnolliset ja mahdolliset muut vaikutukset tullaan käsittelemään kattavasti asianomaisen hallituksen esityksen yhteydessä.

4.4 Vaikutukset hallintoon

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

5 Asian valmistelu

Hallituksen esitys on valmisteltu virkatyönä ulkoasiainministeriössä. Sopimuksen valmisteluun ja sen neuvotteluun on osallistunut edustajia ulkoasiainministeriöstä, oikeusministeriöstä, puolustusministeriöstä sekä työ- ja elinkeinoministeriöstä.

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

Lausunnoissa on puollettu sopimuksen piikaista hyväksymistä ja voimaansaattamista. Lausunnot on otettu huomioon esitystä viimeisteltäessä.

YKSITYISKOHTAISET PERUSTELUT

1 Sopimuksen sisältö ja suhde Suomen lainsäädäntöön

1 artikla. Määritelmät. Sopimuksen 1 artiklassa määritellään sopimuksen soveltamisen kannalta keskeiset käsitteet.

Turvallisuusluokitellulla tiedolla tarkoitetaan sopimuspuolten toisilleen välittämää tai tuottamaa kansallisen lainsäädännön mukaisesti turvallisuusluokiteltua tietoa, asiakirjaa tai aineistoa, joka on merkitty asianmukaisella turvallisuusluokitusmerkinnällä. Turvallisuusluokiteltua tietoa on suojattava luvottomalta ilmaisemiselta, väärinkäytöltä tai kaatoamiselta.

Turvallisuusluokitellulla sopimuksella tarkoitetaan sopimusta tai alihankintasopimusta, taikka näitä edeltäviä neuvotteluja, johon sisältyy turvallisuusluokiteltua tietoa taikka pääsy tällaiseen tietoon. Kohta on sopusoinnussa kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 2 §:n 3 kohdan kanssa.

Lähetävällä sopimuspuolella tarkoitetaan sopimuspuolta sekä sen lainkäyttövaltaan kuuluvaa julkis- tai yksityisoikeudellista oikeushenkilöä, joka luovuttaa turvallisuusluokiteltua tietoa vastaanottavalle sopimuspuolelle. Kyseessä on näin ollen turvallisuusluokitellun tiedon omistaja.

Vastaanottavalla sopimuspuolella tarkoitetaan sopimuspuolta sekä sen lainkäyttövaltaan kuuluvaa julkis- tai yksityisoikeudellista oikeushenkilöä, joka vastaanottaa turvallisuusluokiteltua tietoa lähetävältä sopimuspuolelta.

Kolmannella osapuolella tarkoitetaan valtiota sekä sen lainkäyttövaltaan kuuluvia julkis- tai yksityisoikeudellisia oikeushenkilöitä taikka kansainvälistä järjestöä, joka ei ole tämän sopimuksen sopimuspuoli.

Tiedonsaantitarve tarkoittaa periaatetta, jonka mukaan tietoja saa antaa vain sellaiselle henkilölle, jolla on tarve päästä turvallisuusluokiteltuun tietoon virallisten velvoitteidensa tai tehtäviensä yhteydessä. Vastavantyyppinen määritelmä sisältyy myös kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 6 §:n 3 momenttiin.

2 artikla. Tarkoitus ja soveltamisala. Artiklassa määritellään sopimuksen tarkoituksiksi suojata Suomen ja Slovenian kesken välitetyt turvallisuusluokitellut tiedot. Artiklassa määritellään myös ne toiminnot, joihin sopimusta sovelletaan. Näitä ovat ulko-, puolustus-, turvallisuus ja poliisiasiat sekä teollisuus- tai teknologia-asiat. Rajaturvallisuuden ylläpitämisen katsotaan sisältyvän edellä mainittuihin aloihin. Sopimusta sovelletaan siten vain sellaisten tietojen välittämiseen, jotka koskevat edellä mainittuja toimintoja tai joita tuotetaan tai välitetään näissä yhteyksissä.

Sopimusta ei sovelleta ainoastaan viranomaisten välisiin suhteisiin. Sitä sovelletaan myös sellaisiin, lähinnä taloudellista laatua oleviin sopimuksiin, joissa osapuolena on yksityinen yritys tai yhteisö ja joiden toteuttaminen mukaan lukien myös tarjousvaihe edellyttää turvallisuusluokitellun tiedon ja materiaalin hyödyntämistä.

3 artikla. Toimivaltaiset turvallisuusviranomaiset. Artiklan 1 kappaleessa määritellään kummankin sopimusvaltion toimivaltaiset turvallisuusviranomaiset. Suomessa kansallinen turvallisuusviranomaisena (National Security Authority, NSA) toimii kansainvälisistä tietoturvallisuusvelvoitteista annetun lain mukaan ulkoasiainministeriö, missä tehtävää hoitaa turvallisuusyksikkö. Sloveniassa tehtävää hoitaa Urad Vlade Republike Slovenije za varovanje tajnih podatkov. Artiklan 2 kappale velvoittaa turvallisuusviranomaiset ilmoittamaan toisilleen muista toimivaltaisista turvallisuusviranomaisista, jotka vastaavat sopimuksen täytäntöönpanosta. Suomessa nimettyinä turvallisuusviranomaisina toimivat kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 4 §:n mukaisesti pääesikunta, suojelupoliisi sekä puolustusministeriö. Artiklan 3 kappaleen mukaan sopimuspuolten velvollisuutena on ilmoittaa toisilleen kansallisia turvallisuusviranomaisia koskevista mahdollisista muutoksista.

4 artikla. Turvallisuusluokitukset. Artiklassa määritellään, miten Suomen ja Slovenian turvallisuusluokitusten tasot vastaavat toisiaan. Turvallisuusluokkia on kummassakin

valtiossa neljä. Artiklaan on kirjattu myös kunkin luokan englanninkielinen käännös.

Korkein, ankarimpia tietoturvaluustoi-
menpiteitä vaativa luokka on ”ERITTÄIN
SALAINEN” (STROGO TAJNO). Suo-
messa luokkaan ”erittäin salainen” luetaan
kuuluviksi tiedot, joiden luvaton ilmitulo voi
aiheuttaa erittäin suurta vahinkoa maanpuo-
lustukselle, turvallisuudelle, kansainvälisille
suhteille tai muille yleisille eduille. Suomen
kansainvälisiä suhteita suojaavat julkisuus-
lain 24 §:n 1 momentin 1 ja 2 kohta, maan-
puolustusta momentin 10 kohta ja turvalli-
suutta momentin 5, 8 ja 9 kohdat. Muita mää-
ritelmässä tarkoitettuja yleisiä etuja voivat
olla esimerkiksi valtionjohdon ja valtiovie-
raiden sekä tietojärjestelmien turvallisuusjär-
jestelyjen suojaaminen (24 § 1 mom. 7 koh-
ta) sekä kansantalouden toimivuus (24 § 1
mom. 11 ja 12 kohta).

Toiseksi korkein turvallisuusluokka on
”SALAINEN” (TAJNO). Tähän kuuluvat
Suomessa tiedot, joiden luvaton ilmitulo voi
aiheuttaa merkittävää vahinkoa maanpuolus-
tukselle, turvallisuudelle, kansainvälisille
suhteille tai muille yleisille eduille.

Kolmanneksi korkein turvallisuusluokka
on ”LUOTTAMUKSELLINEN” (ZAUP-
NO), jolla tarkoitetaan Suomessa tietoja, joi-
den luvaton ilmitulo voi aiheuttaa vahinkoa
maanpuolustukselle, turvallisuudelle, kan-
sainvälisille suhteille tai muille yleisille
eduille.

Neljänteen asiakirjaluokkaan ”KÄYTTÖ
RAJOITETTU” (INTERNO) kuuluvat tie-
dot, joiden luvaton ilmitulo voi aiheuttaa
haittaa yleisille eduille tai heikentää viran-
omaisen toimintaedellytyksiä.

*5 artikla. Pääsy turvallisuusluokiteltuun
tietoon.*

Artikla koskee henkilöturvallisuutta. Ar-
tiklan 1 kappaleen mukaan alimpaan turval-
lusluokkaan ”KÄYTTÖ RAJOITETTU”
kuuluvaan tietoon sallitaan pääsy henkilölle,
jolla on tiedonsaantitarve ja jolle on selos-
tettu tähän tietoon liittyvä vastuu ja velvolli-
suudet. Artiklan 2 kappaleen mukaan turval-
lusluokkaan ”LUOTTAMUKSELLI-
NEN” taikka sitä ylempään luokkaan kuulu-
vaan tietoon pääsyn osalta edellytetään edel-
lä olevan lisäksi, että henkilöstä on tehty
kansallisen lainsäädännön mukainen turval-

lususselvitys. Määräys on sopusoinnussa
kansainvälisen tietoturvaluusvelvoitteista
annetun lain 6 §:n 3 momentin kanssa, jossa
sallitaan tietoaaineistoon pääsy vain niille
henkilöille, jotka tarvitsevat tietoja tehtä-
vänsä hoitamiseen. Kansainvälisen tietotur-
valuusvelvoitteen edellyttämä henkilöiden
luotettavuuden varmistaminen toteutetaan
Suomessa turvallisuusselvityksistä annetun
lain sekä kansainvälisistä tietoturvaluus-
velvoitteista annetun lain 11 §:n mukaisesti.
Henkilöturvallisuusselvityksen laatii pää-
esikunta silloin, kun kysymys on puolustus-
hallintoon liittyvästä asiasta, muutoin suoje-
lupoliisi.

Artiklan 3 kappaleen mukaan sopimus-
puolet sitoutuvat tunnustamaan toistensa
turvaluususselvitykset.

*6 artikla. Turvaluusluokitellun tiedon
suojaaminen.* Artiklan 1 kappale sisältää so-
pimuksen keskeisimmän periaatteen, jonka
mukaan sopimuspuolet sitoutuvat antamaan
turvaluusluokitellulle tiedolle samantasoi-
sen suojan kuin vastaavaan omaan kansalli-
seen turvaluusluokkaan luokitellulle tie-
dolleen.

Artiklan 2 kappaleessa luetellaan lähettä-
vän sopimuspuolen toimivaltaisen turval-
lusviranomaisen velvollisuudet turval-
lusluokitellun tiedon suojaamiseksi. Kappa-
leen a kohdan mukaan tämän tulee varmistaa,
että turvaluusluokiteltuun tietoon tehdään
asianmukainen turvaluusluokitusmerkintä
kansallisen lainsäädännön mukaisesti. Kap-
paleen b kohdan mukaan toimivaltaisen tur-
valuusviranomaisen tulee ilmoittaa vas-
taanottavalle sopimuspuolelle mahdollisista
tietoja koskevista luovutusehdoista tai käyt-
törajoituksista sekä mahdollisista myöhem-
mistä luokituksen muutoksista.

Artiklan 3 kappale sisältää puolestaan vas-
taanottavan sopimuspuolen toimivaltaisen
turvaluusviranomaisen velvollisuudet tur-
valuusluokitellun tiedon suojaamiseksi.
Kappaleen a kohdan mukaan tämän tulee
varmistaa, että vastaanotettu turvaluus-
luokiteltu tieto merkitään vastaavalla kansal-
lisella turvaluusluokitusmerkinnällä. Kap-
paleen b kohdan mukaan tämän tulee myös
varmistaa, ettei luokaa muuteta muutoin kuin
lähettävän sopimuspuolen kirjallisella luvalla.

7 artikla. Turvallisuusluokitellun tiedon käytön rajoitukset. Artikla sisältää keskeiset tiedon vastavuoroista suojaamista koskevat sitoumukset.

Artiklan 1 kappaleen mukaan turvallisuusluokiteltua tietoa ei saa käyttää muuhun tarkoitukseen kuin siihen, jota varten se on luovutettu ja lähettävän sopimuspuolen määräämiä rajoituksia noudattaen. Velvoitetta vastaava säännös on kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 6 §:n 2 momentissa.

Artiklan 2 kappale sisältää kiellon luovuttaa turvallisuusluokiteltuja tietoja kolmannelle osapuolelle ilman lähettävän sopimuspuolen toimivaltaisen turvallisuusviranomaisen ennakolta antamaa kirjallista suostumusta. Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 6 §:n 1 momentissa on salassapitovelvollisuutta koskeva erityissäännös, jonka mukaan kansainvälisen tietoturvallisuus sopimuksen mukaisesti turvallisuusluokiteltu tieto on pidettävä salassa.

8 artikla. Turvallisuusluokitellun tiedon välittäminen.

Artikla sisältää määräykset menettelystä siirrettäessä turvallisuusluokiteltuja tietoja sopimuspuolten kesken. Artiklan mukaan tieto välitetään diplomaattiteitse taikka sotilaskanavia tai muita toimivaltaiten turvallisuusviranomaisten hyväksymiä kanavia käyttäen. Turvallisuusluokkaan "KÄYTTÖ RÄJOITETTU" kuuluvaa tietoa voidaan välittää myös postitse tai käyttäen muuta välityspalvelua kansallisen lainsäädännön mukaisesti. Turvallisuusluokkaa vastaavista käsittelyvaatimuksista on säädetty kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 9 §:ssä. Erityissuojattavan tietoa-aineiston käsittelyssä noudatettavista eri turvallisuusluokkia vastaavista turvallisuustoimenpiteistä voidaan säätää valtioneuvoston asetuksella.

9 artikla. Turvallisuusluokitellun tiedon kopiointi, kääntäminen ja hävittäminen.

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

Artiklan 1 kappale sisältää velvoitteen tehdä asianmukainen turvallisuusluokitusmerkintä kaikkiin turvallisuusluokitellun tiedon kopioihin ja käännöksiin. Käännösten ja kopioiden määrä on rajoitettava viralliseen tar-

koitukseen tehtävään vähimmäismäärään. Käännökset on artiklan 2 kappaleen mukaan merkittävä turvallisuusluokiteltua tietoa sisältäviksi myös asianmukaisella käännöskielisellä merkinnällä.

Artiklan 3 kappale sisältää kiellon turvallisuusluokkaan "ERITTÄIN SALAINEN" kuuluvan tiedon kääntämisestä ja kopioinnista ilman aineiston lähettäneen sopimuspuolen turvallisuusviranomaisen siihen etukäteen antamaa kirjallista lupaa. Kansalliset säännökset velvoitteen toteuttamisesta voidaan tarvittaessa säätää kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 9 §:n nojalla.

Artiklan 4 kappaleen mukaan luokkaan "ERITTÄIN SALAINEN" kuuluvaa tietoa ei hävitetä, vaan se palautetaan lähettävälle sopimuspuolelle sen jälkeen, kun sopimuspuolet eivät enää katso sitä tarvittavan. Määräyksellä turvataan tiedon säilyminen esimerkiksi tilanteissa, joissa aineisto tai sen osa on arkistolainsäädännön vuoksi säilytettävä. Turvallisuusluokkaan "SALAINEN" tai sitä alempaan turvallisuusluokkaan kuuluva tieto hävitetään 5 kappaleen mukaan kansallisen lainsäädännön mukaisesti sen jälkeen, kun vastaanottava sopimuspuoli ei enää katso sitä tarvittavan.

10 artikla. Turvallisuusluokitellut sopimukset.

Artikla sisältää määräykset niistä tilanteista varten, joissa toinen sopimuspuoli tekee, taikka antaa luvan oman lainkäyttövaltansa piiriin kuuluvalla hankeosapuolelle tehdä, turvallisuusluokitellun sopimuksen toisen sopimuspuolen lainkäyttövallan piiriin kuuluvan hankeosapuolen kanssa.

Artiklan 1 kappaleen mukaan lähettävän sopimuspuolen turvallisuusviranomaisen on pyynnöstään saatava vastaanottavan sopimuspuolen turvallisuusviranomaiselta ilmoitus siitä, onko hankeosapuolelle annettu vaadittavaa turvallisuusluokkaa vastaava kansallinen turvallisuus selvitys. Määräyksellä pyritään turvaamaan lähettävän sopimuspuolen vapaa harkintavalta hankintasopimusvalmistelussa.

Artiklan 2 kappaleen mukaan kuitenkin silloin, kun kyse on kansainvälisestä avoimesta tarjouskilpailusta, jota ei ole suunnattu erityisesti mihinkään maahan tai yritykseen, vas-

taanottavan sopimuspuolen turvallisuusviranomainen voi toimittaa lähettävän sopimuspuolen turvallisuusviranomaiselle 1 kappaleessa tarkoitetun turvallisuusselvityksen ilman tämän virallista pyyntöä. Määräyksen tarkoituksena on nopeuttaa suomalaisten tai vastavuoroisesti slovenialaisten yritysten pääsyä tarjouksen tekemiseen tarpeelliseen turvallisuusluokiteltuun tietoon, mikä puolestaan tehostaisi yritysten tarjousvalmistelua ja parantaisi niiden kilpailuasemaa.

Artiklan 3 kappale rinnastaa alihankkijat hankeosapuoliin 1 ja 2 kappaleessa mainittujen tietoturvallisuusvaatimusten osalta.

Artiklan 4 kappale mahdollistaa vastaanottavan sopimuspuolen toimivaltaisen turvallisuusviranomaisen tekemät turvallisuustarkastukset organisaatioissaan lähettävän sopimuspuolen ehdotuksesta. Näillä tarkastuksilla pyritään varmistamaan, että organisaatiot täyttävät sopimuksen määräykset. Lähettävän sopimuspuolen turvallisuusviranomaisella on oikeus osallistua kyseisiin tarkastuksiin.

Turvallisuusluokiteltuja sopimuksia koskevat kansalliset säännökset sisältyvät kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 1 § 2 momenttiin (soveltaminen elinkeinonharjoittajaan), 2 §:n 2 kohtaan (erityis-suojattava tietoaineisto), 7 §:ään (vaitiolovelvollisuus ja hyväksikäyttökielto) 12 §:ään (yhteisöturvallisuus selvitys) ja 13 §:ään. Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 13 §:ssä on säännökset hankeosapuolen antamasta sitoumuksesta turvallisuustoimenpiteiden suorittamiseen. Kansallinen sääntely vastaa sopimusvelvoitteen vaatimuksia. Velvoitteen täyttämiseksi tarpeellisesta suomalaisen viranomaisen tietojenanto-oikeudesta säädetään kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 17 §:ssä.

11 artikla. Vierailut. Artikla sisältää määräykset niistä menettelytavoista, joita noudatetaan järjestettäessä sopimuspuolen edustajille tilaisuus tutustua toisen sopimuspuolen sellaisiin toimitiloihin, joissa turvallisuusluokiteltua tietoa kehitetään, käsitellään, tuotetaan tai varastoidaan, taikka turvallisuusluokiteltuja hankkeita toteutetaan.

Artiklan 1 kappaleen mukaan vierailun toteuttaminen toimitiloihin, joissa käsitellään turvallisuusluokiteltua tietoa, edellyttää isäntämaan toimivaltaisen turvallisuusviranomai-

sen ennakolta antamaa lupaa. Artiklan 2 kappaleessa edellytetään, että vierailupyyntö esitetään isäntämaan toimivaltaiselle turvallisuusviranomaiselle vähintään 20 päivää ennen vierailua. Lisäksi 2 kappaleessa on tarkemmat määräykset tiedoista, jotka on sisällytettävä vierailupyyntöön.

Artiklan 3 kappaleessa todetaan, että kii-reellisissä tapauksissa toimivaltaiset turvallisuusviranomaiset voivat sopia lyhyemmästä vierailupyynnön esittämisajasta.

Artiklan 4 kappaleen mukaan toimivaltaiset turvallisuusviranomaiset voivat laatia luettelot henkilöistä, joilla on lupa toistuviin vierailuihin. Luettelo on voimassa enintään 12 kuukautta, jonka jälkeen sen voimassaoloa voidaan pidentää enintään 12 kuukaudella. Luettelon hyväksymisen jälkeen asianomaiset organisaatiot, joita vierailu koskee, voivat järjestää vierailuja suoraan keskenään. Artiklan 5 kappaleen mukaan vierailijan saama turvallisuusluokiteltu tieto katsotaan tämän sopimuksen mukaiseksi turvallisuusluokitteluksi tiedoksi.

Vierailujen toteuttamiseen liittyvät säännökset ovat kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 18 §:ssä.

12 artikla. Turvallisuusyhteistyö.

Artikla sisältää määräykset sopimuspuolten viranomaisten välisestä yhteistyöstä sopimuksen täytäntöönpanon varmistamiseksi.

Artiklan 1 kappaleen mukaan sopimuspuolten toimivaltaiset turvallisuusviranomaiset antavat toisilleen tiedoksi turvallisuusluokitellun tiedon suojaamiseen sovellettavat kansalliset turvallisuusnorminsa, - menettelynsä ja -käytäntönsä. Toimivaltaiset turvallisuusviranomaiset voivat myös vierailla toistensa luona järjestelmiin tutustumiseksi. Vierailuilla pyritään selventämään toisen sopimuspuolen turvallisuusluokitellun tiedon turvaamista koskevia menettelyjä.

Artiklan 2 kappaleessa edellytetään, että toimivaltaiset turvallisuusviranomaiset ilmoittavat toisilleen poikkeuksellisista turvallisuusriskeistä, jotka voivat vaarantaa turvallisuusluokitellun tiedon. Artiklan 3 kappaleen mukaan toimivaltaiset turvallisuusviranomaiset avustavat pyynnöstä toisiaan turvallisuus selvityksiin liittyvissä menettelyissä. Artiklan 4 kappale velvoittaa turvallisuusviranomaiset ilmoittamaan viipymättä turvallisuus selvityk-

siä koskevista muutoksista. Artiklan 5 kappaleessa sallitaan sopimuspuolten turvallisuusviranomaisten vaihtaa suoraan keskenään operatiivisia tietoja ja/tai tiedustelutietoja kansallisen lainsäädännön mukaisesti. Artiklan 6 kappaleen mukaan sopimuksen kattamassa yhteistyössä käytetään englannin kieltä.

13 artikla. Tietoturvaloukkaus. Artiklan 1 kappaleen mukaan sopimuspuolen toimivaltainen turvallisuusviranomaisella on velvollinen ilmoittamaan viipymättä toisen sopimuspuolen toimivaltaiselle turvallisuusviranomaiselle epäilyistä tai todetusta tietoturvaloukuksesta. Se sopimuspuoli, jonka lainkäyttövaltaan asia kuuluu, toteuttaa 2 kappaleen mukaan kansallisen lainsäädäntönsä mukaisesti kaikki mahdolliset toimenpiteet rajoittaakseen tietoturvan loukkausten seurauksia sekä estääkseen loukkausten jatkumisen. Toinen sopimuspuoli avustaa tarvittaessa tutkimuksessa. Toiselle sopimuspuolelle toimitetaan joka tapauksessa tieto tutkimuksen tuloksista sekä loukkauksen johdosta toteutetuista toimenpiteistä. Artiklan tarkoittamien velvoitteiden täyttämiseen panemiseksi tarpeelliset säännökset sisältyvät kansainvälisistä tietoturvaluusvelvoitteista annetun lain 19 §:ään.

14 artikla. Kustannukset. Artiklan mukaan kumpikin sopimuspuoli vastaa itse omista sopimuksen täytäntöönpanosta aiheutuneista kustannuksistaan.

15 artikla. Tulkitseminen ja riitojen ratkaiseminen.

Artiklan mukaan kaikki sopimuksen tulkitaan tai soveltamiseen liittyvät sopimuspuolten väliset riidat ratkaistaan yksinomaan sopimuspuolten välisissä neuvotteluissa.

16 artikla. Loppumääräykset. Artiklassa on sopimuksen voimaantuloa, muuttamista, ja irtisanomista koskevat määräykset. Sopimus on tehty toistaiseksi ja sitä voidaan muuttaa sopimuspuolten yhteisestä sopimuksesta. Sopimuksen irtisanominen tulee voimaan kuuden kuukauden kuluessa irtisanomisilmoituksen vastaanottamisesta. Sopimuksen irtisanomisesta riippumatta kaikki sopimuksen mukaisesti luovutettu turvallisuusluokiteltu tieto suojataan edelleen sopimuksen määräyksiä noudattaen, kunnes lähettävä sopimuspuoli vapauttaa vastaanottavan sopimuspuolen tästä velvoitteesta.

2 Lakiehdotuksen perustelut

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

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

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

3 Voimaantulo

Suomen ja Slovenian välisen sopimuksen 16 artiklan 1 kappaleen mukaan kumpikin sopimuspuoli ilmoittaa toiselle sopimuspuolelle, kun sopimuksen voimaantulon edellyttämät kansallisen lainsäädännön mukaiset vaatimukset on saatettu päätökseen. Sopimus tulee voimaan toiseksi seuraavan kuukauden ensimmäisenä päivänä jälkimmäisen ilmoituksen vastaanottamisesta.

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

4 Eduskunnan suostumuksen tarpeellisuus ja käsittelyjärjestys

4.1 Eduskunnan suostumuksen tarpeellisuus

Perustuslain 94 §:n 1 momentin mukaan eduskunta hyväksyy sellaiset valtiosopimukset ja muut kansainväliset velvoitteet, jotka sisältävät lainsäädännön alaan kuuluvia mää-

räyksiä. Perustuslakivaliokunnan tulkinta-käytännön mukaan määräys on luettava lainsäädännön alaan kuuluvaksi, jos se koskee jonkin perustuslaissa turvatun perusoikeuden käyttämistä tai rajoittamista, jos määräys muutoin koskee yksilön oikeuksien ja velvollisuuksien perusteita, jos määräyksen tarkoituksesta asiasta on perustuslain mukaan säädetty lailla, tai jos määräyksessä tarkoitusta asiasta on jo voimassa lain säännöksiä taikka siitä on Suomessa vallitsevan käsityksen mukaan säädetty 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 1 artiklassa määritellään, mitä tarkoitetaan turvallisuusluokitellulla tiedolla ja turvallisuusluokitelluilla sopimuksilla. Sopimuksen 2 artiklassa määritellään puolestaan sopimuksen tarkoitus ja soveltamisala. Koska nämä sopimusmääräykset vaikuttavat joko suoraan tai välillisesti sopimuksen lainsäädännön alaan kuuluvien aineellisten määräysten tulkintaan ja soveltamiseen, ne edellyttävät eduskunnan hyväksymistä (PeVL 6/2001 vp).

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

Turvallisuusluokiteltua tietoa koskeva käyttörajoitus ja turvallisuusluokiteltua tietoa saavia henkilöitä koskeva rajoitus on ilmaistu sopimuksen 5 artiklassa. Siinä määrätään sopimuspuolten velvollisuudesta teettää asianmukainen turvallisuusselvitys henkilöistä, joilla on tai saattaa olla pääsy sopimuksessa tarkoitettuun turvallisuusluokiteltuun tietoon. Turvallisuusselvitysten laadinnassa on otettava huomioon perustuslain 10 §:n 1 momentissa säädetty yksityiselämän suoja ja velvollisuus säätää henkilötietojen suojasta lailla.

Suomessa turvallisuusselvityksen kohteena olevista henkilöistä sekä selvityksessä sovellettavasta menettelystä on säädetty turvallisuusselvityksistä annetussa laissa.

Sopimuksen 6 ja 7 artiklassa määrätään sopimuksen soveltamisalan piiriin kuuluvan turvallisuusluokitellun tiedon suojaamiseksi tarvittavista kansallisista toimenpiteistä, jotka rajoittavat turvallisuusluokitellun tiedon välittämistä, käyttämistä ja pääsyä siihen. Sopimuspuolet ovat 6 artiklan mukaan velvollisia antamaan tälle turvallisuusluokitellulle tiedolle saman suojan kuin omalle vastaavaan turvallisuusluokkaan kuuluvalla tiedolle, mikä edellyttää vastaanotetun turvallisuusluokitellun tiedon merkitsemistä asianmukaisesti. Vastaanottavan sopimuspuolen on 7 artiklassa ilmaistun pääsäännön mukaan pidettävä turvallisuusluokiteltu tieto salassa.

Suomessa viranomaisten asiakirjojen julkisuus on pääsääntö. Jokaisella on perustuslain 12 §:n 2 momentin mukaan oikeus saada tieto viranomaisen julkisesta asiakirjasta. Tätä oikeutta voidaan rajoittaa välttämättömistä syistä vain lailla. Yleisesti sovellettavat säännökset salassapito- ja luokitusmerkinnästä on säädetty julkisuuslain 25 §:ssä. Lain 25 §:n 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. Julkisuuslain säännöksistä poiketen kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 6 §:n 1 momentin mukaan erityissuojattava tietoaineisto on pidettävä salassa. Lisäksi samaisen 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. Sopimusmääräykset asettavat näin ollen Suomen lainsäädäntöä tiukemmat vaatimukset turvallisuusluokitellun tiedon merkitsemiselle. Määräykset edellyttävät eduskunnan hyväksymistä.

Sopimuksen 8 artiklassa on määräykset turvallisuusluokitellun tiedon välittämisestä ja 9 artiklassa turvallisuusluokitellun tiedon kääntämisestä, kopioinnista ja hävittämisestä. Turvallisuusluokkaa vastaavista käsittelyvaatimuksista on säädetty kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 9 §:ssä. Erityissuojattavan tietoaineiston käsittelyssä noudatettavista eri turvallisuusluokkia vastaavista turvallisuustoimenpiteistä voidaan säätää valtioneuvoston asetuksella.

Sopimuksen 10 artiklassa on määräykset turvallisuusluokitelluista sopimuksista ja niihin tarvittavista turvallisuus selvityksistä. Yhteisöturvallisuus selvitystä koskevat säännökset sisältyvät kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 12 ja 13 §:ään.

Sopimuksen 11 artiklassa on määräykset toisen sopimuspuolen luonnollisten henkilöiden vierailuista isäntämaana toimivan sopimuspuolen tiloihin, joissa käsitellään turvallisuusluokiteltua tietoa. Sopimuspuolen edustajien vierailuiden tarkoituksena on varmistaa sopimuksen tarkoituksen toteuttaminen turvallisuusluokiteltujen tietojen asianmukaiseksi suojaamiseksi. Tähän vierailuoikeuteen ei sisälly sellaista julkista vallan käyttöä ja tarkastusoikeutta, joka olisi ristiriidassa perustuslain kanssa (PeVL 179/1997). Sopimusmääräys luo välillisesti myös yksityisille tilausten saajille velvollisuuden sallia vierailut omiin toimitiloihinsa. Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 18 §:ssä on vastaavat säännökset vierailuja koskevan sopimusmääräyksen täytäntöönpanoon liittyvistä seikoista.

Sopimuksen 13 artiklassa edellytetään, että sopimuspuolen toimivaltainen turvallisuusviranomainen ilmoittaa välittömästi toisen sopimuspuolen toimivaltaiselle turvallisuusviranomaiselle, jos tietoturvaloukkauksen todetaan tapahtuneen taikka sitä epäillään. Sopimuspuolten on tutkittava turvallisuusluokitellun tiedon suojaamista koskevien säännösten rikkominen sekä ryhdyttävä mahdollisuuksien mukaan toimenpiteisiin myös kolmannessa maassa tapahtuneen tietoturvaloukkauksen suhteen. Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 19 §:ssä säädetään kansallisen turvallisuusviranomaiselle kuuluvista velvoitteista sopimusmääräyksissä tarkoitetuissa tilanteissa.

4.2 Käsittelyjärjestys

Käsittelyjärjestyksen kannalta merkityksellisiä sopimusmääräyksiä sisältyy sopimuksen 5 -7 artiklaan, jotka asettavat rajoituksia turvallisuusluokitellun tiedon tai materiaalin julkisuudelle. Sopimusmääräykset ovat merkityksellisiä perustuslain 12 §:n 2 momentin suojaaman, julkisuusperiaatteelle rakentuvan tiedonsaantioikeuden kannalta. Tätä tiedonsaantioikeutta saa rajoittaa vain lailla ja vain välttämättömistä syistä. Tällaisena välttämättömänä syynä voidaan pitää sen turvaamista, että Suomi ja suomalaiset yritykset voivat osallistua sellaisiin kansainvälisiin sekä Suomen ja Slovenian kahdenkeskisiin toimintoihin ja hankkeisiin, joiden toteuttaminen edellyttää arkaluonteisen salassa pidettävien tietojen vaihtoa. Salassapitoa koskeva erityissäännös on otettu kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 6 §:ään.

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

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

että Eduskunta hyväksyisi Ljubljanassa 6 päivänä toukokuuta 2008 Suomen tasavallan ja Slovenian tasavallan välillä turvallisuusluokitellun tiedonvaihtamisesta ja vastavuoroisesta suojaamisesta tehdyn sopimuksen.

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

Laki

Slovenian kanssa turvallisuusluokitellun tiedon vaihtamisesta ja vastavuoroisesta suojaamisesta tehdyn sopimuksen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta

Eduskunnan päätöksen mukaisesti säädetään:

1 §
Ljubljanassa 6 päivänä toukokuuta 2008 Suomen tasavallan ja Slovenian tasavallan välillä turvallisuusluokitellun tiedon vaihtamisesta ja vastavuoroisesta suojaamisesta tehdyn sopimuksen lainsäädännön alaan kuu-

luvat määräykset ovat lakina voimassa sellaisina kuin Suomi on niihin sitoutunut.

2 §
Tämän lain voimaantulosta säädetään tasavallan presidentin asetuksella.

Helsingissä 3 päivänä lokakuuta 2008

Tasavallan Presidentti

TARJA HALONEN

Ulkoasiainministeri *Alexander Stubb*

*Sopimusteksti***Sopimus**

**Suomen tasavallan hallituksen
ja
Slovenian tasavallan hallituksen
välillä
turvallisuusluokitellun tiedon
vaihtamisesta
ja
vastavuoroisesta suojaamisesta**

Suomen tasavallan hallitus ja Slovenian tasavallan hallitus, jäljempänä "sopimuspuolet", jotka kansallisten etujen ja turvallisuuden vuoksi haluavat varmistaa sellaisen turvallisuusluokitellun tiedon suojaamisen, jota sopimuspuolet tai niiden lainkäyttövaltaan kuuluvat julkis- ja yksityisoikeudelliset oikeushenkilöt vaihtavat keskenään, ovat sopineet seuraavasta:

1 artikla*Määritelmät*

Tässä sopimuksessa seuraavilla käsitteillä on seuraava merkitys:

turvallisuusluokiteltu tieto: tieto, asiakirja tai aineisto, jota sopimuspuolet välittävät tai tuottavat keskenään missä tahansa muodossa jommankumman sopimuspuolen kansallisen lainsäädännön mukaisesti ja joka on suojattava luvattomalta ilmaisemiselta, väärinkäytöltä tai katoamiselta ja on nimetty sellaiseksi sekä merkitty asianmukaisesti;

turvallisuusluokiteltu sopimus: sopimus tai alihankintasopimus, sopimusta edeltävät neuvottelut mukaan lukien, johon sisältyy turvallisuusluokiteltua tietoa tai liittyy pääsy tällaiseen tietoon;

lähettävä sopimuspuoli: sopimuspuoli, mukaan lukien sen lainkäyttövaltaan kuuluvat julkis- tai yksityisoikeudelliset oikeushenkilöt, joka luovuttaa turvallisuusluokiteltua tietoa vastaanottavalle sopimuspuolelle;

vastaanottava sopimuspuoli: sopimuspuoli, mukaan lukien sen lainkäyttövaltaan kuuluvat

Agreement

**between
the Government of the Republic of
Finland
and
the Government of the Republic of
Slovenia
on
the Exchange and Mutual Protection
of Classified Information**

The Government of the Republic of Finland and the Government of the Republic of Slovenia, hereinafter referred to as the "Parties", wishing to ensure the protection of Classified Information exchanged between the Parties or between public and private entities under their jurisdiction, in respect of national interests and security, have agreed on the following:

Article 1*Definitions*

For the purposes of this Agreement these terms mean the following:

Classified Information: Any information, document or material, regardless of its form, which is transmitted or generated between the Parties under the national legislation of either Party, requires protection against unauthorised disclosure, misappropriation or loss and is designated as such and marked appropriately.

Classified Contract: A contract or a sub-contract, including pre-contractual negotiations, which contains Classified Information or involves access to it.

Originating Party: The Party, including any public or private entities under its jurisdiction, which releases Classified Information to the Recipient Party.

Recipient Party: The Party, including any public or private entities under its jurisdiction,

julkis- tai yksityisoikeudelliset oikeushenkilöt, joka vastaanottaa turvallisuusluokiteltua tietoa lähettävältä sopimuspuolelta;

kolmas osapuoli: valtio, mukaan lukien sen lainkäyttövaltaan kuuluvat julkis- tai yksityisoikeudelliset oikeushenkilöt, tai kansainvälinen järjestö, joka ei ole tämän sopimuksen sopimuspuolena;

tiedonsaantitarve: periaate, jonka mukaan pääsy turvallisuusluokiteltuun tietoon voidaan sallia henkilölle ainoastaan hänen virallisten velvoitteidensa tai tehtäviensä yhteydessä.

2 artikla

Tarkoitus ja soveltamisala

Tämän sopimuksen tarkoituksena on suojata turvallisuusluokiteltua tietoa, jota sopimuspuolet antavat toisilleen pääasiassa ulko-, puolustus-, turvallisuus- ja poliisiasioissa sekä teollisuus- tai teknologia-asioissa tai jota välitetään turvallisuusluokiteltujen sopimusten täytäntöönpanon taikka valmistelun yhteydessä tai jota syntyy taikka tuotetaan tämän sopimuksen soveltamisalaan kuuluvan toiminnan yhteydessä.

3 artikla

Toimivaltaiset turvallisuusviranomaiset

1. Sopimuspuolet ovat nimenneet seuraavat kansalliset turvallisuusviranomaiset vastaamaan tämän sopimuksen kaikkien näkökohtien yleisestä täytäntöönpanosta ja asiaankuuluvasta valvonnasta:

Suomen tasavallassa:
Ulkoasiainministeriö, turvallisuusyksikkö

Slovenian tasavallassa:
Urad Vlade Republike Slovenije za varovanje tajnih podatkov

2. Kansalliset turvallisuusviranomaiset ilmoittavat toisilleen muut toimivaltaiset turvallisuusviranomaiset, jotka vastaavat tämän sopimuksen täytäntöönpanosta.

3. Sopimuspuolet ilmoittavat toisilleen kansallisten turvallisuusviranomaistensa mahdolliset myöhemmät muutokset.

tion, which receives Classified Information from the Originating Party.

Third Party: A state, including any public or private entities under its jurisdiction, or an international organisation that is not a Party to this Agreement.

Need-to-Know: A principle by which access to Classified Information may be granted to an individual only in connection with his/her official duties or tasks.

Article 2

Purpose and Scope of Application

The purpose of this Agreement is to protect Classified Information provided by one Party to the other Party mainly for purposes of foreign affairs, defence, security and police matters as well as industrial or technological matters, or transmitted within the context of the implementation or preparation of Classified Contracts, or arising or produced within the context of an activity falling within the scope of application of this Agreement.

Article 3

Competent Security Authorities

1. The National Security Authorities designated by the Parties as responsible for the general implementation and the relevant controls of all aspects of this Agreement are:

In the Republic of Finland:
Ulkoasiainministeriö, turvallisuusyksikkö

In the Republic of Slovenia:
Urad Vlade Republike Slovenije za varovanje tajnih podatkov

2. The National Security Authorities shall notify each other of any other Competent Security Authorities that are responsible for the implementation of this Agreement.

3. The Parties shall inform each other of any subsequent changes of the National Security Authorities.

4 artikla

Article 4

*Turvallisuusluokitukset**Security Classifications*

1. Tämän sopimuksen mukaisesti luovutettavaan turvallisuusluokiteltuun tietoon merkitään asianmukainen turvallisuusluokka sopimuspuolten kansallisen lainsäädännön mukaisesti.

2. Kansalliset turvallisuusluokitusmerkinnät vastaavat toisiaan seuraavasti:

1. Classified Information released under this Agreement shall be marked with the appropriate security classification level under the national legislation of the Parties.

2. The equivalence of the national security classification markings is as follows:

Suomen tasavalta	Slovenian tasavalta	Englanninkielinen käännös
ERITTAIN SALAINEN	STROGO TAJNO	TOP SECRET
SALAINEN	TAJNO	SECRET
LUOTTAMUKSELLINEN	ZAUPNO	CONFIDENTIAL
KÄYTTÖ RAJOITETTU	INTERNO	RESTRICTED

5 artikla

Article 5

*Pääsy turvallisuusluokiteltuun tietoon**Access to Classified Information*

1. Pääsy turvallisuusluokkaan KÄYTTÖ RAJOITETTU/INTERNO kuuluvaan tietoon sallitaan ainoastaan henkilöille, joilla on tiedonsaantitarve ja joille on selostettu heidän vastuunsa ja velvollisuutensa.

2. Pääsy turvallisuusluokkaan LUOTTAMUKSELLINEN/ZAUPNO ja sitä ylempään turvallisuusluokkaan kuuluvaan tietoon sallitaan ainoastaan henkilöille, joilla on tiedonsaantitarve, joista on tehty kansallisen lainsäädännön mukainen turvallisuusselvitys ja joille on annettu lupa saada tällaista tietoa sekä selostettu heidän vastuunsa ja velvollisuutensa.

3. Sopimuspuolet tunnustavat vastavuoroisesti toistensa turvallisuusselvitykset. Sopimuksen 4 artiklan 2 kappaletta sovelletaan tämän mukaisesti.

1. Access to information classified as KÄYTTÖ RAJOITETTU/INTERNO shall be limited to persons who have a Need-to-Know and who have been briefed accordingly.

2. Access to information classified as LUOTTAMUKSELLINEN/ZAUPNO and above shall be limited to persons who have a Need-to-Know and who, in accordance with national legislation, have been security cleared and authorized to have access to such information as well as briefed accordingly.

3. The Parties shall mutually recognise their respective security clearances. Paragraph 2 of Article 4 shall apply accordingly.

6 artikla

Article 6

*Turvallisuusluokitellun tiedon suojaaminen**Protection of Classified Information*

1. Sopimuspuolet antavat tässä sopimuksessa tarkoitettulle turvallisuusluokitellulle tiedolle samantasoisien suojan kuin omalle vastaavaan turvallisuusluokkaan kuuluvalla tiedolle.

1. The Parties shall afford to Classified Information referred to in this Agreement the same protection as to their own information of the corresponding level of security classification.

2. Lähettävän sopimuspuolen toimivaltainen turvallisuusviranomainen

a) varmistaa, että turvallisuusluokiteltuun tietoon tehdään asianmukainen turvallisuusluokitusmerkintä sen kansallisen lainsäädännön mukaisesti, ja

b) ilmoittaa vastaanottavalle sopimuspuolelle

– mahdollisista tietoa koskevista luovutusehdoista tai käyttörajoituksista ja

– mahdollisista myöhemmistä luokituksen muutoksista.

3. Vastaanottavan sopimuspuolen toimivaltainen turvallisuusviranomainen

a) varmistaa, että turvallisuusluokiteltuun tietoon tehdään vastaavat turvallisuusluokitusmerkinnät 4 artiklan 2 kappaleen mukaisesti, ja

b) varmistaa, ettei turvallisuusluokkaa muuteta muutoin kuin lähettävän sopimuspuolen kirjallisella luvalla.

7 artikla

Turvallisuusluokitellun tiedon käytön rajoitukset

1. Vastaanottava sopimuspuoli saa käyttää turvallisuusluokiteltua tietoa ainoastaan siihen tarkoitukseen, jota varten se on luovutettu, ja lähettävän sopimuspuolen määrittämiä rajoituksia noudattaen.

2. Vastaanottava sopimuspuoli ei saa luovuttaa turvallisuusluokiteltua tietoa kolmannelle osapuolelle ilman lähettävän sopimuspuolen kirjallista suostumusta.

8 artikla

Turvallisuusluokittelun tiedon välittäminen

1. Sopimuspuolet välittävät turvallisuusluokitellun tiedon diplomaattiteitse tai sotilaskanavia taikka muita toimivaltaisten turvallisuusviranomaistensa hyväksymiä kanavia käyttäen kansallisen lainsäädännön mukaisesti.

2. Turvallisuusluokkaan KÄYTTÖ RAJOITETTU/INTERNO kuuluva tieto voidaan välittää myös postitse tai käyttäen muuta välityspalvelua kansallisen lainsäädännön mukaisesti.

2. The Competent Security Authority of the Originating Party shall:

a) ensure that the Classified Information is marked with an appropriate security classification marking in accordance with its national legislation, and

b) inform the Recipient Party

– of any conditions of release or limitations on the use of the Classified Information, and

– of any subsequent changes in the classification.

3. The Competent Security Authority of the Recipient Party shall:

a) ensure that the Classified Information is marked with an equivalent classification marking in accordance with Paragraph 2 of Article 4, and

b) ensure that the classification level is not changed unless authorized in writing by the Originating Party.

Article 7

Restriction of use of Classified Information

1. The Recipient Party shall use the Classified Information only for the purpose for which it has been delivered and within the limitations stated by the Originating Party.

2. The Recipient Party shall not release Classified Information to a Third Party without a written consent of the Originating Party.

Article 8

Transmission of Classified Information

1. Classified Information shall be transmitted between the Parties through diplomatic or military channels or through other channels approved by their Competent Security Authorities in accordance with national legislation.

2. Information classified as KÄYTTÖ RAJOITETTU/INTERNO may be transmitted also by post or another delivery service in accordance with national legislation.

9 artikla

*Turvallisuusluokitellun tiedon kopiointi,
kääntäminen ja hävittäminen*

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

2. Kaikkiin käännöksiin tehdään asianmukainen käännöskielen merkintä siitä, että käännökset sisältävät lähetettävän sopimuspuolen turvallisuusluokiteltua tietoa.

3. Merkinnällä ERITTÄIN SALAINEN/STROGO TAJNO varustettua turvallisuusluokiteltua tietoa saa kääntää tai kopioida ainoastaan lähetettävän sopimuspuolen kirjallisella luvalla.

4. Merkinnällä ERITTÄIN SALAINEN/STROGO TAJNO varustettua turvallisuusluokiteltua tietoa ei hävitetä. Se palautetaan lähetävälle sopimuspuolelle sen jälkeen, kun sopimuspuolet eivät enää katso sitä tarvittavan.

5. Turvallisuusluokkaan SALAINEN/TAJNO tai sitä alempaan turvallisuusluokkaan kuuluva tieto hävitetään sen jälkeen, kun vastaanottava sopimuspuoli ei enää katso sitä tarvittavan, kansallisen lainsäädännön mukaisesti.

10 artikla

Turvallisuusluokitellut sopimukset

1. Jos lähetettävän sopimuspuolen toimivaltainen turvallisuusviranomainen aikoo sallia neuvottelut turvallisuusluokitellun sopimuksen tekemiseksi vastaanottavan sopimuspuolen lainkäyttövaltaan kuuluvan hankeosapuolen kanssa, tämän viranomaisen on pyynnöstä saatava kaikki asiaankuuluvat turvallisuustodistukset vastaanottavan sopimuspuolen toimivaltaiselta turvallisuusviranomaiselta.

2. Jos on kyse avoimesta turvallisuusluokittelusta tarjouskilpailusta, vastaanottavan sopimuspuolen toimivaltainen turvallisuusviranomainen voi antaa asiaankuuluvat turvallisuustodistukset lähetettävän sopimuspuolen toimivaltaiselle turvallisuusviranomaiselle myös pyytämättä.

Article 9

*Reproduction, Translation and Destruction
of Classified Information*

1. All reproductions and translations shall bear appropriate security classification markings and they shall 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/ STROGO TAJNO shall be translated or reproduced only upon the written permission of the Originating Party.

4. Classified Information marked ERITTÄIN SALAINEN/ STROGO TAJNO shall not be destroyed. It shall be returned to the Originating Party after it is no longer considered necessary by the Parties.

5. Information classified as SALAINEN/TAJNO or below shall be destroyed after it is no longer considered necessary by the Recipient Party, in accordance with national legislation.

Article 10

Classified Contracts

1. If the Competent Security Authority of the Originating Party intends to permit negotiations for concluding a Classified Contract with a contractor under the jurisdiction of the Recipient Party, it shall, on request, obtain all relevant security certificates from the Competent Security Authority of the Recipient Party.

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

3. Alihankkijoihin sovelletaan samoja turvallisuusvaatimuksia, mukaan lukien asianmukaiset todistukset, kuin turvallisuusluokitellun pääsopimuksen tehneeseen hankeosapuoleen.

4. Lähettävän sopimuspuolen toimivaltainen turvallisuusviranomainen voi ehdottaa, että vastaanottavan sopimuspuolen toimivaltainen turvallisuusviranomainen tekee organisaatioissa turvallisuustarkastuksia, joilla varmistetaan organisaatioiden olevan tämän sopimuksen mukaisia, ja se voi osallistua näihin tarkastuksiin

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

4. The Competent Security Authority of the Originating Party may propose and participate in security inspections carried out by the Competent Security Authority of the Recipient Party at facilities to ensure their compliance with this Agreement.

11 artikla

Vierailut

1. Vierailut, jotka edellyttävät pääsyä turvallisuusluokiteltuun tietoon, sallitaan isäntä-sopimuspuolen toimivaltaisen turvallisuusviranomaisen ennakolta antamalla luvalla.

2. Vierailupyynnö esitetään asianomaiselle toimivaltaiselle turvallisuusviranomaiselle vähintään 20 päivää ennen vierailun alkamista, ja siinä ilmoitetaan seuraavat tiedot:

a) vierailijan nimi, syntymäaika ja -paikka, kansallisuus ja henkilöllisyystodistuksen tai passin numero;

b) vierailijan asema ja tiedot vierailijan edustamasta työnantajasta;

c) tiedot hankkeesta, johon vierailija osallistuu;

d) tarvittaessa vierailijan turvallisuusselvityksen voimassaoloaika ja taso;

e) vierailun kohteena olevan organisaation nimi, osoite, puhelin- tai telefaxnumero, sähköpostiosoite ja yhteyshenkilö;

f) vierailun tarkoitus sekä siihen liittyvän turvallisuusluokitellun tiedon korkein turvallisuusluokituksen taso;

g) vierailun ajankohta ja kesto; toistuvien vierailujen osalta ajanjakso, jolle vierailut ajoittuvat;

h) päiväys ja lähettävän toimivaltaisen turvallisuusviranomaisen allekirjoitus.

3. Kiireellisissä tapauksissa toimivaltaiset turvallisuusviranomaiset voivat sopia lyhyemmästä vierailupyynnön esittämisen määräajasta.

4. Turvallisuusviranomaiset voivat sopia sellaisten vierailijoiden luettelosta, joilla on oikeus toistuviin vierailuihin. Luettelo on

Article 11

Visits

1. Visits necessitating access to Classified Information shall be subject to prior permission of the Competent Security Authority of the host Party.

2. A request for visit shall be submitted to the relevant Competent Security Authority at least 20 days prior to the commencement of the visit and shall include the following:

a) the visitor's name, date and place of birth, nationality and ID card/passport number;

b) the visitor's position, with a specification of the employer which the visitor represents;

c) a specification of the project in which the visitor participates;

d) the validity and level of the visitor's security clearance, if required;

e) the name, address, phone/fax number, e-mail and point of contact of the facility to be visited;

f) the purpose of the visit, including the highest level of Classified Information to be involved;

g) the date and duration of the visit. In the case of recurring visits the total period covered by the visits shall be stated;

h) the date and signature of the sending Competent Security Authority.

3. In urgent cases, the Competent Security Authorities can agree on a shorter period.

4. The Competent Security Authorities may agree on a list of visitors entitled to recurring visits. The list shall be valid for an initial pe-

aluksi voimassa enintään 12 kuukautta, ja sen voimassaoloa voidaan pidentää enintään 12 kuukaudella. Toistuvia vierailuja koskeva pyyntö esitetään tämän artiklan 2 kappaleen mukaisesti. Kun luettelo on hyväksytty, asianomaiset organisaatiot voivat järjestää vierailuja suoraan keskenään.

5. Vierailijan saama turvallisuusluokiteltu tieto katsotaan tämän sopimuksen mukaiseksi turvallisuusluokitelluksi tiedoksi.

12 artikla

Turvallisuusyhteistyö

1. Saavuttaakseen keskenään vertailukelpoiset turvallisuustasot ja säilyttääkseen ne vertailukelpoisina toimivaltaiset turvallisuusviranomaiset ilmoittavat pyynnöstä toisilleen turvallisuusluokitellun tiedon suojaamiseen sovellettavat kansalliset turvallisuusnorminsa, menettelynsä ja käytäntönsä. Tätä varten toimivaltaiset turvallisuusviranomaiset voivat vierailla toistensa luona.

2. Toimivaltaiset turvallisuusviranomaiset ilmoittavat toisilleen poikkeuksellisista turvallisuusriskeistä, jotka voivat vaarantaa luovutetun turvallisuusluokitellun tiedon.

3. Toimivaltaiset turvallisuusviranomaiset avustavat pyynnöstä toisiaan turvallisuusselvityksiin liittyvissä menettelyissä kansallisen lainsäädännön mukaisesti.

4. Toimivaltaiset turvallisuusviranomaiset ilmoittavat viipymättä toisilleen muutoksista, jotka koskevat vastavuoroisesti tunnustettuja turvallisuusselvityksiä.

5. Sopimuspuolten turvallisuusviranomaiset voivat vaihtaa suoraan keskenään operatiivisia tietoja ja/tai tiedustelutietoja kansallisen lainsäädännön mukaisesti.

6. Tämän sopimuksen mukaisessa yhteistyössä käytetään englannin kieltä.

13 artikla

Tietoturvaloukkaus

1. Sopimuspuolet ilmoittavat viipymättä toisilleen epäilyistä tai todetusta turvallisuusluokitellun tiedon tietoturvan loukkaamisesta tai vaarantumisesta.

2. Se sopimuspuoli, jonka lainkäyttövaltaan asia kuuluu, toteuttaa kansallisen lainsäädän-

riod not exceeding 12 months and may be extended for a further period of time not exceeding 12 months. A request for recurring visits shall be submitted in accordance with Paragraph 2 of this Article. Once a list has been approved, visits may be arranged directly between the facilities involved.

5. Any Classified Information acquired by a visitor shall be considered as Classified Information under this Agreement.

Article 12

Security co-Operation

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

2. The Competent Security Authorities shall inform each other of exceptional security risks that may endanger the released Classified Information.

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

4. The Competent Security Authorities shall promptly inform each other about any changes in mutually recognized security clearances.

5. The security services of the Parties may exchange operative and/or intelligence information directly in accordance with national legislation.

6. The co-operation under this Agreement shall be effected in the English language.

Article 13

Breach of Security

1. Each Party shall immediately notify the other Party of any suspicion or discovery of a breach or compromise of the security of Classified Information.

2. The competent Party shall undertake all possible appropriate measures under its na-

tönsä mukaisesti kaikki mahdolliset asianmukaiset toimenpiteet rajoittaakseen tämän artiklan 1 kappaleessa tarkoitetun tietoturvan loukkaamisen tai vaarantumisen seurauksia ja estääkseen tietoturvaloukkauksen jatkumisen. Toinen sopimuspuoli antaa pyynnöstä tutkinta-apua; sille ilmoitetaan tutkimuksen tuloksista sekä tietoturvaloukkauksen johdosta toteutetuista toimenpiteistä.

14 artikla

Kustannukset

Sopimuspuolet vastaavat omista kustannuksistaan, jotka aiheutuvat tämän sopimuksen täytäntöönpanosta.

15 artikla

Tulkitseminen ja riitojen ratkaiseminen

Sopimuspuolten väliset riidat, jotka koskevat tämän sopimuksen tulkintaa tai soveltamista, ratkaistaan yksinomaan sopimuspuolten välisillä neuvotteluilla.

16 artikla

Loppumääräykset

1. Tämä sopimus tehdään määräämättömäksi ajaksi. Se on hyväksyttävä sopimuspuolten kansallisia oikeudellisia menettelyjä noudattaen ja tulee voimaan toiseksi seuraavan kuukauden ensimmäisenä päivänä sen jälkeen, kun sopimuspuolista jälkimmäinen on saanut ilmoituksen siitä, että sopimuksen voimaantulon edellyttämät vaatimukset on täytetty.

2. Sopimuspuoli voi milloin tahansa irtisanoa tämän sopimuksen kirjallisesti. Tällöin sopimus lakkaa olemasta voimasta 6 kuukauden kuluttua päivästä, jona toinen sopimuspuoli saa irtisanomisilmoituksen.

3. Tämän sopimuksen irtisanomisesta riippumatta kaikki sopimuksen mukaisesti luovutettu turvallisuusluokiteltu tieto suojataan edelleen sopimuksen määräyksiä noudattaen, kunnes lähettävä sopimuspuoli vapauttaa vastaanottavan sopimuspuolen tästä velvoitteesta.

tional legislation so as to limit the consequences of the breach or compromise referred to in Paragraph 1 of this Article and to prevent further violations. On request, the other Party shall provide investigative assistance; it shall be informed of the outcome of the investigation and the measures undertaken due to the violation.

Article 14

Expenses

Each Party shall bear its own expenses incurred in the course of implementation of this Agreement.

Article 15

Interpretation and Dispute Settlement

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

Article 16

Final Provisions

1. This Agreement is concluded for an indefinite period of time. It is subject to approval in accordance with the national legal procedures of the Parties and shall enter into force on the first day of the second month following receipt of the later notification between the Parties that the necessary requirements for this Agreement to enter into force have been met.

2. Each Party shall have the right to terminate this Agreement in writing at any time. In such a case the validity of the Agreement shall expire 6 months following the day on which the termination notice was received by the other Party.

3. Notwithstanding the termination of this Agreement, all Classified Information delivered under this Agreement shall continue to be protected in accordance with the provisions stated in this Agreement until the Originating Party dispenses the Recipient Party from this obligation.

4. Tätä sopimusta voidaan milloin tahansa muuttaa sopimuspuolten kirjallisella suostumuksella. Muutokset tulevat voimaan tämän artiklan 1 kappaleen mukaisesti.

5. Tämä sopimus ei rajoita sopimuspuolten oikeuksia ja velvoitteita, jotka perustuvat muihin kansainvälisiin sopimuksiin.

6. Tämän sopimuksen täytäntöönpanoksi voidaan tehdä täytäntöönpanojärjestelyjä.

Tehty Ljubljanassa 6 päivänä toukokuuta 2008 kahtena alkuperäiskappaleena, suomen, sloveenin ja englannin kielellä, kaikkien tekstien ollessa yhtä todistusvoimaiset. Jos syntyy tulkintaeroja, englanninkielinen teksti on ratkaiseva.

Tämän vakuudeksi allekirjoittaneet, siihen asianmukaisesti valtuutettuina, ovat allekirjoittaneet tämän sopimuksen.

Suomen tasavallan
hallituksen puolesta

Slovenian tasavallan
hallituksen puolesta

4. This Agreement may be amended at any time by written consent of both Parties. Such amendments shall enter into force in accordance with Paragraph 1 of this Article.

5. This Agreement does not prejudice the rights and obligations of the Parties arising from other international agreements.

6. Implementing arrangements may be concluded for the implementation of this Agreement.

Done in Ljubljana on May 6th, 2008 in two originals in the Finnish, Slovenian and English languages, each text being equally authentic. In case of different interpretation the English text shall prevail.

In witness whereof the undersigned, being duly authorised thereto, have signed this Agreement.

On behalf of the Government of the
Republic of Finland

On behalf of the Government of the
Republic of Slovenia