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

ESITYKSEN PÄÄASIALLINEN SISÄLTÖ

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

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

Sopimus tulee voimaan toiseksi seuraavan kuukauden ensimmäisenä päivänä sen jälkeen, kun on otettu vastaan jälkimmäinen ilmoitus, jolla osapuolet ilmoittavat toisilleen, että sopimuksen voimaansaattamiseksi tarvittavat kansalliset toimenpiteet on saatettu loppuun. Sopimuksen voimaansaattamislaki on tarkoitettu tulemaan voimaan valtioneuvoston asetuksella säädettävänä ajankohtana samaan aikaan kuin sopimus tulee Suomen osalta voimaan.

SISÄLLYS

YLEISPERUSTELUT

1 Johdanto

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

Kansainväliseen yhteistyöhön liittyviin asiakirjoihin sisältyy toisinaan sellaisia salassa pidettäviä tietoja, joiden luvaton paljastuminen voi aiheuttaa merkittävää ja laajalle ulottuvaa vahinkoa keskeisille yleisille eduille. Tällaisten aineistojen asianmukaisesta käsittelystä on sen vuoksi pidettävä erityistä huolta. Kysymys on Suomen luotettavuudesta kansainvälisen yhteistyön osapuolena. Kansainvälinen tietoturvallisuusyhteistyö, johon Suomikin osallistuu, käsittää perinteisesti diplomaattiseen toimintaan samoin kuin puolustushallintojen väliseen yhteistyöhön liittyvän ei-julkisen tiedonvaihdon suojaamisen. Välittömän valtiovastuun piiriin kuuluvien kysymysten lisäksi kansainvälisillä tietoturvallisuusvelvoitteilla on kuitenkin kasvava merkitys myös taloudellisen, teollisen ja teknologisen yhteistyön kannalta, joiden puitteissa yhä useammat yritystason hankkeet edellyttävät turvallisuusluokitellun tiedon hyödyntämistä. Näin etenkin silloin, kun kyse on sellaisesta viranomaisen hankinnasta, jossa valtion suojattuja tietoja on annettava yritykselle kaupallisen sopimuksen toteuttamista varten. Tällaisia ovat perinteisesti olleet erityisesti puolustusalan hankinnat, mutta nykyään yhä enenevässä määrin myös muilla sektoreilla tapahtuvat hankinnat, kuten esimerkiksi informaatioteknologian ja ydinvoima-alan hankinnat.

Pyrkimyksistä huolimatta ei kuitenkaan ole osoittautunut mahdolliseksi toteuttaa tietoturvallisuusalan monenkeskistä yleissopimusta. Pääasiallinen syy tähän on kansallisten lainsäädäntöjen ja hallintorakenteiden ja -tapojen eroavaisuudet, jotka puolestaan heijastelevat tietoturvallisuuden sensitiivisyyttä osana kansallista kokonaisturvallisuutta. Edellä sanotusta poikkeuksena on kuitenkin Tanskan, Suomen, Islannin, Norjan ja Ruotsin välillä turvallisuusluokitellun tiedon vastavuoroisesta suojaamisesta ja vaihtamisesta tehty yleinen turvallisuussopimus (SopS 11 ja 12/2013).

Yleissopimuksen puuttuminen on pakottanut valtiot, Suomi mukaan luettuna, etsimään kahdenvälisiä sopimusratkaisuja. Suomi on tehnyt ensimmäisen kahdenvälisen tietoturvallisuussopimuksensa Saksan liittotasavallan kanssa vuonna 2004. Sopimus tuli voimaan 16 päivänä heinäkuuta 2004 (SopS 96 ja 97/2004). Vuotta myöhemmin allekirjoitettiin Suomen ja Ranskan välinen sopimus, joka puolestaan tuli voimaan 1 päivänä elokuuta 2005 (SopS 66 ja 67/2005). Kumpikin suuri Euroopan unionin (EU) jäsen on Suomelle tärkeä yhteistyökumppani niin turvallisuushallinnon kuin taloudellisen vuorovaikutuksenkin aloilla. Tietoturvallisuustarpeiden painottumista enenevässä määrin myös taloudelliseen toimintaan ilmentää Suomen ja Euroopan Avaruusjärjestön (ESA) välinen yhteistyösopimus, jäljempänä ESA:n tietoturvallisuussopimus, niin ikään vuodelta 2004 (SopS 94 ja 95/2004). Sopimuksen eräs keskeinen tavoite on turvata Suomen elinkeinoelämän mahdollisuudet osallistua tasavertaisesti muiden jäsenmaiden kanssa ESA:n turvallisuusluokiteltuihin tarjouskilpailuihin. Tietoturvallisuussopimus on tehty myös Länsi-Euroopan unionin (WEU) kanssa (SopS 41 ja 42/1998) ja Eurooppalaisen puolustusmateriaaliyhteistyöjärjestön (OCCAR) (SopS 109 ja 110/2008) ja Pohjois-Atlantin liiton

(Nato) (SopS 7 ja 8/2013) kanssa. Mainittujen sopimusten lisäksi Suomi on tehnyt voimassaolevan tietoturvallisuussopimuksen Slovakian (SopS 116 ja 117/2007), Viron (SopS 12 ja 13/2008), Italian (SopS 23 ja 24/2008), Latvian (SopS 33 ja 34/2008), Puolan (SopS 46 ja 47/2008), Bulgarian (SopS 116 ja 117/2008), Slovenian (SopS 22 ja 23/2009), Tšekin (SopS 53 ja 54/2009), Espanjan (SopS 38 ja 39/2010), Amerikan yhdysvaltojen (SopS 41 ja 42/2013), Ison-Britannian (SopS 49 ja 50/2013), Luxemburgin (SopS 59 ja 60/2013)ja Sveitsin (SopS 88 ja 89/2014) kanssa. Suomi on 10 päivänä toukokuuta 2012 hyväksynyt EU:n jäsenvaltioiden välillä toukokuussa 2011 allekirjoitetun sopimuksen turvallisuusluokitellun tiedon suojaamisesta. Lisäksi Suomi on tehnyt soveltamisalaltaan suppeamman tietoturvallisuussopimuksen Israelin kanssa puolustus- tai turvallisuushallintojen kesken välitetystä turvallisuusluokitellusta tiedosta (SopS 34 ja 35/2012).

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

2 Nykytila

2.1 Laki kansainvälisistä tietoturvallisuusvelvoitteista

Lain yleinen soveltamisala

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

Lakia kansainvälisistä tietoturvallisuusvelvoitteista sovelletaan erityissuojattaviin tietoaineistoihin. Näillä tarkoitetaan salassa pidettäviä asiakirjoja ja materiaaleja, jotka on toimitettu Suomen viranomaiselle ja joiden luovuttaja on kansainvälisen, Suomea sitovan sopimuksen tai muun kansainvälisen velvoitteen mukaisesti tehnyt niihin turvallisuusluokkaa koskevan merkinnän. Määräysvalta luovutettuun tietoon säilyy luovutuksen jälkeenkin aineiston luovuttaneella valtiolla. Lakia voidaan soveltaa vain, jos kansainvälinen sopimus on saatettu Suomessa voimaan perustuslaissa säädetyllä tavalla tai jos kysymys on Suomea muutoin sitovasta kansainvälisestä velvoitteesta.

Lain soveltamisalan piiriin kuuluvia erityissuojattavia tietoaineistoja ovat lisäksi Suomen viranomaisen tai lain soveltamisalan piiriin kuuluvan elinkeinonharjoittajan laatimat asiakirjat, joista ilmenee Suomeen toimitettuihin asiakirjoihin sisältyviä tai materiaalista saatavissa olevia tietoja. Lain soveltamisalan piiriin kuuluvat niin ikään asiakirjat ja materiaalit, jotka on Suomessa tuotettu erityissuojattavan tietoaineiston pohjalta. Lakia ei sovelleta pelkästään Suomen kansallista tietoa sisältävien asiakirjojen tai niiden osien salassapitoon tai luokitukseen.

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

Vireillä olevat muutokset

Uusi turvallisuusselvityslaki (726/2014) tulee voimaan 1 päivänä tammikuuta 2015. Lailla kumotaan turvallisuusselvityksistä annettu laki (177/2002). Samalla kansainvälisistä tietoturvallisuusvelvoitteista annetun lain henkilöturvallisuusselvityksiä koskeva 11 §, yhteisöturvallisuusselvityksiä koskeva 12 § ja turvallisuustodistuksia koskeva 14 § muutetaan (Laki kansainvälisistä tietoturvallisuusvelvoitteista annetun lain muuttamisesta, 731/2014). Kansainvälisistä tietoturvalli-

suusvelvoitteista annettuun lakiin lisätään muutoksenhakua koskeva 20 a § ja elinkeinonharjoittajan antamaa sitoumusta koskeva 13 § kumotaan, mutta vastaava säännös sisällytetään turvallisuusselvityslakiin (40 §). Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain muutokset tulevat voimaan niin ikään 1 päivänä tammikuuta 2015.

Lain suhde julkisuuslainsäädäntöön

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

Lain soveltaminen elinkeinonharjoittajiin

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

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

Elinkeinonharjoittaja voi pyytää yhteisöturvallisuusselvityksen ja arvion tekemistä voidakseen osallistua toisen valtion viranomaisen tai siinä kotipaikkaansa pitävän yrityksen järjestämään tarjouskilpailuun (12 §:n 2 mom.). Vastaava säännös sisältyy uuteen turvallisuusselvityslakiin (33 §:n 2 mom.). Säännöksen tarkoituksena on turvata suomalaisten yritysten kilpailumahdollisuudet hankinnoissa silloinkin, kun hankintaan sovellettavissa olevaa kansainvälistä tietoturvallisuussopimusta ei ole. Useimmat valtiot kuitenkin edellyttävät kahdenvälisen tietoturvallisuussopimuksen olemassa oloa ulkomaisen turvallisuustodistuksen hyväksymiseksi.

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

Lain täytäntöönpanoviranomaiset

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

Henkilöturvallisuutta koskevien turvallisuusselvitysten, jäljempänä henkilöturvallisuusselvitys, laadinnasta huolehtivat Suojelupoliisi ja pääesikunta (11 §). Yhteisöturvallisuusselvityksen laadinta kuuluu lain mukaan Suojelupoliisille, paitsi silloin, kun kyse

on puolustukseen liittyvästä hankinnasta, jolloin selvitysten tekemisestä huolehtii pääesikunta (12 §). Vastaava viranomaisten toimivaltaa koskeva säännös sisältyy uuteen turvallisuusselvityslakiin (9 §). Kun edellä selostetut muutokset kansainvälisistä tietoturvallisuusvelvoitteista annettuun lakiin tulevat voimaan, kansainvälisessä tietoturvallisuusvelvoitteessa edellytetty henkilöturvallisuusselvitys ja yritysturvallisuusselvitys laaditaan siten kuin uudessa turvallisuusselvityslaissa säädetään. Henkilö- ja yritysturvallisuusselvitystodistuksen antaa tällöin kansallinen turvallisuusviranomainen, jollei erityisestä syystä muuta johdu (muutettu 11 § ja 12 §).

Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 5 §:n 2 momentin mukaan kansallinen turvallisuusviranomainen ja tehtävään määrätyt turvallisuusviranomaiset voivat sen estämättä, mitä muun muassa toimivallasta yhteisöturvallisuusselvitysten laadinnasta säädetään, sopia tietyn tehtävän tai tehtäväkokonaisuuden hoitamisesta toisen turvallisuusviranomaisen lukuun, jos järjestely on tarpeen tehtävien hoitamiseksi tarkoituksenmukaisesti, taloudellisesti ja joutuisasti. Viestintävirasto on lain 4 §:n 1 momentissa (885/2010) määrätty turvallisuusviranomaiseksi, jonka tehtävänä on toimia asiantuntijana tietojärjestelmien ja tietoliikennejärjestelyjen turvallisuutta koskevissa asioissa.

Laissa kansainvälisistä tietoturvallisuusvelvoitteista on säännökset viranomaisia ja elinkeinonharjoittajaa koskevasta tiedonantovelvollisuudesta (16 §). Säännösten tarkoituksena on varmistaa, että toimivaltaiset turvallisuusviranomaiset voisivat saada niille kuuluvien tehtävien hoitamiseksi tarpeelliset tiedot. Viranomaiset voivat myös salassapitovelvollisuuden estämättä antaa kansainväliseen tietoturvallisuusvelvoitteeseen perustuvaa yhteistyötä varten salassa pidettäviä tietoja ulkomaiselle sopimuspuolelle (17 §). 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 (18 §).

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

Tietojen salassapito ja käytön sääntely

Erityissuojattava tietoaineisto on pidettävä salassa, jollei kansainvälisestä tietoturvallisuusvelvoitteesta muuta johdu (6 §:n 1 mom.). Salassapitovelvollisuus koskee myös elinkeinonharjoittajaa tämän ollessa osapuolena turvallisuusluokitellussa sopimuksissa. Suomen tekemissä, käytännössä kahdenvälisissä sopimuksissa, jotka koskevat eri maiden viranomaisten välistä salassa pidettävien tietojen vaihtoa, on säännönmukaisesti määräys, joka rajoittaa luovutettujen tietojen käyttöä. Kyseisen määräyksen mukaisesti erityissuojattavaa tietoaineistoa saa käyttää ja luovuttaa vain siihen tarkoitukseen, jota varten se on annettu, jollei se, joka on määritellyt aineiston turvallisuusluokan, ole antanut muuhun suostumustaan. Erityissuojattavien tietoaineistojen käyttöä koskee siten vahva käyttötarkoitussidonnaisuus.

Turvallisuusluokittelu ja – toimenpiteet

Laissa säädetään velvollisuudesta merkitä erityissuojattavaan tietoaineistoon sen turvallisuusluokka. Tietoaineistoon tehty merkintä turvallisuusluokasta osoittaa, minkälaisia toimenpiteitä on toteutettava aineistoa käsiteltäessä (8 §). Mitä korkeampaan turvallisuusluokkaan aineisto kuuluu, sitä tiukempia tietoturvallisuustoimenpiteitä edellytetään. Laissa on yleinen velvoite toteuttaa tietoaineiston käsittelyssä sen turvallisuusluokkaa koskevia käsittelymääräyksiä sekä valtuus säätää erityissuojattavan tietoaineiston käsittelyssä noudatettavista eri turvallisuusluokkia vastaavista turvallisuustoimenpiteistä valtio-

neuvoston asetuksella (9 §). Tietoturvallisuudesta valtionhallinnossa annetun valtioneuvoston asetuksen (681/2010), jäljempänä *tietoturvallisuusasetus*, 11 §:ssä on säädetty turvallisuusluokitusmerkintää koskevista erityissäännöksistä ja 12 §:ssä turvallisuusluokituksen vastaavuudesta.

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

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

Henkilöstöturvallisuus

Kansainvälisessä tietoturvallisuusvelvoitteessa edellytetty henkilöturvallisuusselvitys tehdään siten kuin turvallisuusselvityksistä annetussa laissa (177/2002) ja sen nojalla säädetään. Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain muutosten tultua voimaan kansainvälisissä tietoturvallisuusvelvoitteissa edellytetty henkilöturvallisuusselvitys laaditaan siten kuin uudessa turvallisuusselvityslaissa säädetään. Siten esimerkiksi selvityksen kohteena olevan henkilön oikeudet määräytyvät sanotun lain mukaisesti.

Turvallisuusselvityksistä annetun lain 10 §:n 2 momentin mukaan turvallisuusselvitykseen ei saa sisällyttää selvityksen laatineen viranomaisen arviota selvityksen kohteena olevan henkilön luotettavuudesta tai sopivuudesta virkaan tai tehtävään, ellei lain 9 §:ssä tarkoitettu valtiosopimus tai muu kansainvälinen velvoite tätä edellytä. Koska pääsääntönä on, että turvallisuusselvitys ei sisällä arviota henkilön luotettavuudesta, laissa kansainvälisistä tietoturvallisuusvelvoitteista on erikseen säädetty henkilön luotettavuuden arvioinnista. Tällaisen arvion tekee turvallisuusselvityksen perusteella kansallinen turvallisuusviranomainen tai, jos turvallisuusviranomaisten välillä on niin sovittu, tehtävään määrätty turvallisuusviranomainen (11 §:n 3 mom.). Arvioinnin perusteella annetaan henkilöturvallisuutta koskeva todistus (Personnel Security Clearance Certificate). Se toimitetaan tavanomaisimmin sopimuspuolen turvallisuusviranomaiselle sopimuksen osoittamalla tavalla. Laissa on myös säännökset todistuksen antamisesta henkilölle itselleen (14 §).

Myös uuden turvallisuusselvityslain mukaan henkilöturvallisuusselvitykseen ei saa sisällyttää viranomaisen arviota selvityksen kohteena olevan henkilön nuhteettomuudesta, luotettavuudesta tai sopivuudesta virkaan tai tehtävään (42 §). Lain 43 §:n mukaan kansallinen turvallisuusviranomainen antaa kansainvälisen tietoturvallisuusvelvoitteiden toteuttamiseksi tarpeellisen henkilöturvallisuusselvitystodistuksen siten kuin kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa säädetään. Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain muutoksen tultua voimaan selvityksen 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 (muutettu 11 §:n 1 momentti). Todistuksen antamiseen koskevaan arvioon sekä sen voimassaoloon ja peruuttamiseen sovelletaan turvallisuusselvityslakia (muutettu 11 §:n 2 momentti).

Yhteisöturvallisuusselvitys

Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 12 §:ssä säädetään yhteisöturvallisuusselvityksistä ja arvioista. Yhteisöturvallisuusselvityksellä varmistetaan elinkeinonharjoittajan toimitilojen ja käsittelykäytäntöjen asianmukaisuus sekä henkilöstön osaaminen. Elinkeinonharjoittajan luotettavuuden arvioinnilla varmistutaan erityisesti siitä, kuinka hyvin tämä pystyy huolehtimaan turvallisuusluokiteltujen tietojen suojaamisesta. Yhteisöturvallisuusmenettely ja siihen perustuva arvio toteutetaan pääosin elinkei-

nonharjoittajalta itseltään saatujen tietojen perusteella sekä tämän toimitilojen turvallisuuden kartoituksella, ja tarvittavista toimenpiteistä huolehditaan elinkeinonharjoittajan kanssa tehtävän sopimuksen avulla. Selvityksen laatii Suojelupoliisi. Pääesikunta huolehtii tehtävästä kuitenkin silloin, kun kysymys on puolustukseen liittyvästä hankinnasta. Selvitystä laadittaessa on otettava huomioon laissa yksilöidyt seikat, muun muassa se, miten suojataan turvallisuusluokiteltuja tietoja oikeudettomalta ilmitulolta, muuttamiselta ja hävittämiseltä, ja miten estetään asiaton pääsy tiloihin, joissa turvallisuusluokiteltuja tietoja käsitellään tai joissa harjoitetaan turvallisuusluokitellussa sopimuksessa tarkoitettua toimintaa. Viestintävirasto laatii tarvittaessa osana yhteisöturvallisuusselvitystä selvityksen ja arvion siitä, täyttävätkö elinkeinonharjoittajan tietojärjestelmät ja tietoliikenteen järjestelyt kansainvälisistä tietoturvallisuusvelvoitteista johtuvat vaatimukset.

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

Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain muutosten tultua voimaan kansainvälisissä tietoturvallisuusvelvoitteissa edellytetty yritysturvallisuusselvitys laaditaan siten kuin uudessa turvallisuusselvityslaissa säädetään. Yritysturvallisuusselvitystodistuksen antaa kuitenkin kansallinen turvallisuusviranomainen, jollei erityisestä syystä muuta johdu. Selvityksen 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 (muutettu 12 §:n 1 momentti). Todistuksen voimassaoloon ja peruuttamiseen sovelletaan turvallisuusselvityslakia (muutettu 12 §:n 2 momentti).

2.2 Turvallisuusselvityksiä koskeva lainsäädäntö

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

Turvallisuusselvitys voidaan tehdä virkaan tai tehtävään hakeutuvasta, tehtävään tai koulutukseen otettavasta taikka virkaa tai tehtävää hoitavasta henkilöstä, ja se voi olla perusmuotoinen, laaja tai suppea. 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 tyhjentävästi.

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

Tammikuussa 2015 voimaan tulevan uuden turvallisuusselvityslain tarkoituksena on parantaa mahdollisuuksia ennakolta ehkäistä toimintaa, joka voi vahingoittaa valtion turvallisuutta, maanpuolustusta, Suomen kansainvälisiä suhteita, yleistä turvallisuutta tai muuta niihin verrattavaa yleistä etua tai erittäin merkittävää yksityistä taloudellista etua. Uudessa laissa on säännökset mm. selvityksen kohteen asemasta ja oikeudesta (2 luku), toimivaltaisista viranomaisista ja niiden harkintavallan ohjauksesta (3 luku), henkilöturvallisuusselvityksestä (4 luku) yritysturvallisuusselvityksistä (5 luku), turvallisuusselvitysmenettelyn päättämisestä (6 luku), turvallisuusselvitysrekisteristä (7 luku) sekä turvallisuusselvityksen ja turvallisuusselvitystodistuksen voimassaolosta (8 luku).

Uuden turvallisuusselvityslain mukaan Suojelupoliisilla on yleinen toimivalta päättää turvallisuusselvityksen tekemisestä (9 §:n 1 momentti). Pääesikunta laatii henkilöturvallisuusselvityksen niissä tapauksissa, joissa selvityksen kohde toimii tai sen on tarkoitus toimia puolustusvoimissa taikka hoitaa puolustusvoimien antamaa tehtävää tai joissa selvitys liittyy puolustusvoimien toimintaan tai hankintoihin. Pääesikunta laatii yritysturvallisuusselvityksen, jos yritys hoitaa tai sen on tarkoitus hoitaa puolustusvoimien antamaa tehtävää ja yrityksestä, joka liittyy puolustusvoimien hankintoihin (9 §:n 3 momentti). Viestintävirasto laatii yritysselvityksen osana tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden tasoa koskevan selvityksen (9 §:n 4 momentti).

Myös uuden turvallisuusselvityslain mukaan henkilöturvallisuusselvitys on tarkan muotosidonnaista ja henkilöturvallisuusselvitys voidaan tehdä vain kohteena olevan henkilön etukäteisellä kirjallisella suostumuksella (5 §). Selvitys voi olla suppea, perusmuotoinen tai laaja (14 §). Lain 15 §:ssä määritellään henkilöturvallisuusselvityksen hakemiseen oikeutetut. Turvallisuusselvityksessä käytettävä tietopohja laajenee ja selvityksessä voidaan käyttää myös tiettyjä ulkomaan viranomaisen rekistereihin talletettuja tietoja (25§). Turvallisuusselvitysmenettelyssä käytetyt rekisterit on laissa lueteltu tyhjentävästi.

Uudessa laissa on säännökset myös yritysturvallisuusselvityksistä. Lain 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 yritykseen ja sen toimitiloihin sekä sen tietojärjestelmiin ja tietoliikennejärjestelyihin kohdistuneen tarkastuksen avulla, miten yritys voi huolehtia turvallisuusjärjestelyistä (38 §:n 1 momentti). Käytännössä yritysturvallisuusselvityksen laatimiseen osallistuu kaksi viranomaista, koska Viestintäviraston tehtävänä on huolehtia tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista. Toimivaltaisten viranomaisten käytettävissä olevin keinoin selvitetään, miten yritys voi huolehtia erilaisista tietoturvallisuuteen kuuluvista seikoista. Toimivaltainen viranomainen voi yritysturvallisuusselvitystä ja sen perusteella annettavaa todistusta laatiessaan edellyttää, että elinkeinonharjoittaja sitoutuu huolehtimaan tietoturvallisuustason säilyttämisestä (40 §).

3 Esityksen tavoitteet ja keskeiset ehdotukset

Esityksen tavoitteena on hankkia eduskunnan hyväksyntä sopimukselle. Sopimuksen tavoitteena on varmistua siitä, että Suomen Kroatiaan luovuttamaa turvallisuusluokiteltua tietoa suojataan ja käsitellään asianmukaisesti. Sopimuksen tavoitteena on myös edistää Suomen mahdollisuuksia vastaanottaa Kroatian turvallisuusluokiteltua tietoa ja parantaa maiden välistä yhteistyötä tietoturvallisuuden alalla. Lisäksi sopimuksen tarkoituksena on turvata suomalaisten yritysten mahdollisuudet osallistua sellaisiin kansainvälisiin sekä Suomen ja Kroatian välisiin hankkeisiin, joiden toteuttaminen saattaa edellyttää turvallisuusluokiteltujen tietojen vaihtoa ja parantaa näin suomalaisten yritysten kilpailukykyä. 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 Kroatiasta 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 Kroatian välisen sopimuksen mukaisia erityissuojattavia tietoaineistoja ovat aineistot, joita Kroatia pitää salassa pidettävinä ja jotka se on määritellyt ja merkinnyt korkean tietoturvallisuuden tasoa edellyttäviksi. Sopimuksen 5 artiklassa määrätään turvallisuusluokitellun tiedon salassapidosta. Artiklan 9 a kohdan mukaan vastaanottava osapuoli välittää turvallisuusluokiteltua tietoa kolmannelle osapuolelle ainoastaan luovuttavan osapuolen kirjallisella ennakkosuostumuksella. Tämä merkitsee poikkeusta julkisuuslain yleistä etua koskevista salassapitosäännöksistä, joissa salassapito on useimmissa tapauksissa riippuvainen siitä, minkälaisia vaikutuksia tietojen antamisella olisi suojattavalle edulle. Ilman tietoturvallisuussopimustakin Kroatian Suomeen luovuttamat turvallisuusluokitellut asiakirjat pidettäisiin säännönmukaisesti salassa kansainvälisiä suhteita koskevina julkisuuslain 24 §:n 1 momentin 2 kohdan perusteella, mikä merkitsee, että tietoturvallisuussopimus ei rajoita kansalaisen tiedonsaantia enempää kuin mitä se julkisuuslain mukaan on.

Merkittävimpänä erona on se, että viranomaisella ei olisi kansainvälisessä tietoturvallisuusvelvoitteessa tarkoitettuun asiakirjaan kohdistuvaa tiedonsaantipyyntöä ratkaistessaan velvollisuutta erikseen perustella tiedon antamisesta aiheutuvaa vahinkoa. Tiedonsaantipyyntö olisi muutoin käsiteltävä julkisuuslain mukaisesti. Jos syntyy epäselvyyttä luokituksen oikeellisuudesta tai siitä, mitkä asiakirjassa olevat tiedot ovat johtaneet luokitusmerkintään, viranomaisen on otettava yhteyttä asiakirjan laatineeseen osapuoleen.

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

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

4.2 Vaikutukset elinkeinoelämään

Sopimus antaa suomalaisille yrityksille mahdollisuuden saada sellaisia tilauksia tai osallistua sellaisiin hankkeisiin, joiden toteuttaminen edellyttää pääsyä Kroatian turvallisuusluokiteltuihin tietoihin. Vastaavasti sopimus antaa kroatialaisille 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 Kroatiassa 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 turvallisuusvi-

ranomaisen ja määrättyjen turvallisuusviranomaisten niitä tehtäviä, jotka kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 4 §:n mukaisesti kuuluvat näille viranomaisille.

5 Asian valmistelu

Hallituksen esitys on valmisteltu ulkoasiainministeriössä. Sopimuksen valmisteluun ja neuvotteluihin on osallistunut edustajia ulkoasiainministeriöstä, oikeusministeriöstä, puolustusministeriöstä ja Suojelupoliisista. Esityksestä on pyydetty lausunnot liikenne- ja viestintäministeriöltä, oikeusministeriöltä, puolustusministeriöltä, sisäministeriöltä, työ- ja elinkeinoministeriöltä, valtiovarainministeriöltä, Suojelupoliisilta ja Viestintävirastolta. Lausunnot on saatu liikenne- ja viestintäministeriöltä, puolustusministeriöltä, sisäministeriöltä, sekä Suojelupoliisilta. Sisäministeriö on lausunnossaan pyytänyt tarkentamaan hallituksen esityksen perusteluja poliisin tutkinta- ja tiedustelutiedon osalta. Lausunto on otettu huomioon sopimuksen tavoitetta koskevan 1 artiklan yksityiskohtaisissa perusteluissa. Lausunnoissa on puollettu sopimuksen hyväksymistä ja voimaansaattamista.

YKSITYISKOHTAISET PERUSTELUT

1 Sopimuksen sisältö ja suhde Suomen lainsäädäntöön

1 artikla. *Tavoite.* Artiklassa määritellään sopimuksen tavoitteeksi varmistaa sellaisen turvallisuusluokitellun tiedon suojaaminen, jota tuotetaan tai vaihdetaan osapuolten kesken. Sopimuksen johdannossa osapuolten välisinä yhteistyöaloina luetellaan ulko-, puolustus-, turvallisuus- ja poliisiasiat sekä tiedeelinkeino ja teknologia-asiat. 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 1 kohdassa on turvallisuusluokitellun tiedon määritelmä. Sopimus koskee missä tahansa muodossa olevaa tietoa, joka on suojattava tietoturvaloukkauksilta ja luokiteltu luovuttavan osapuolen kansallisten säädösten ja määräysten mukaisesti. Kohta on sopusoinnussa kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 2 §:n 1 kohdan määritelmän kanssa.

Artiklan 2 kohdan mukaan tiedonsaantitarpeella tarkoitetaan tarvetta päästä turvallisuusluokiteltuun tietoon tietyssä virallisessa asemassa tai tietyn tehtävän suorittamiseksi.

Artiklan 3 kohdan mukaan tietoturvaloukkauksella tarkoitetaan missä tahansa muodossa tapahtuvaa turvallisuusluokitellun tiedon luvatonta ilmaisemista tai muuttamista, väärinkäyttöä, vahingoittamista tai hävittämistä taikka muuta sellaista tekoa tai laiminlyöntiä, jonka johdosta tieto voi menettää luottamuksellisuutensa, eheytensä tai käytettävyytensä.

Artiklan 4 kohdan mukaan turvallisuusluokalla tarkoitetaan luokkaa, joka kansallisten säädösten ja määräysten mukaisesti ilmaisee niiden rajoitusten tason, joilla osapuolet rajoittavat pääsyä turvallisuusluokiteltuun tietoon, sekä osapuolten tälle tiedolle antaman suojan vähimmäistason.

Artiklan 5 kohdan mukaisesti luovuttavalla osapuolella tarkoitetaan osapuolta, joka luovuttaa turvallisuusluokiteltua tiedon tai jonka alaisuudessa turvallisuusluokiteltu tieto tuotetaan.

Artiklan 6 kohdan mukaisesti vastaanottavalla osapuolella tarkoitetaan osapuolta, jolle luovuttavan osapuolen turvallisuusluokiteltu tieto välitetään. Määritelmä kattaa myös tämän osapuolen lainkäyttövaltaan kuuluvat julkis- tai yksityisoikeudelliset oikeushenkilöt ja luonnolliset henkilöt.

Artiklan 7 kohdan mukaan kansallisella turvallisuusviranomaisella tarkoitetaan kansallista viranomaista, joka vastaa sopimuksen täytäntöönpanosta ja sen valvonnasta.

Artiklan 8 kohdan mukaan toimivaltaisella turvallisuusviranomaisella tarkoitetaan kansallista turvallisuusviranomaista, määrättyä turvallisuusviranomaista tai kansallista tietoturvaviranomaista tai muuta sellaista kansallista viranomaista, joka panee täytäntöön sopimusta kansallisten säädösten ja määräysten mukaisesti.

Artiklan 9 kohdan mukaan hankeosapuolella tarkoitetaan luonnollista henkilöä tai oikeushenkilöä, jolla on oikeudellinen kelpoisuus tehdä sopimuksia;

Artiklan 10 kohdan mukaan turvallisuusluokitellulla sopimuksella tarkoitetaan kahden tai useamman hankeosapuolen välistä sopimusta, johon sisältyy pääsy turvallisuusluokiteltuun tietoon tai jonka täytäntöönpano edellyttää tätä. Kohta on sopusoinnussa kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 2 §:n 1 kohdan määritelmän kanssa.

Artiklan 11 kohdan mukaan henkilöturvallisuusselvityksellä tarkoitetaan toimivaltaisen turvallisuusviranomaisen kansallisten säädösten ja määräysten mukaisesti tekemää arviota, jonka mukaan luonnolliselle henkilölle voidaan sallia pääsy turvallisuusluokiteltuun tietoon.

Artiklan 12 kohdan mukaan yhteisöturvallisuusselvityksellä tarkoitetaan toimivaltaisen turvallisuusviranomaisen tekemää arviota, jolla vahvistetaan kyseisen osapuolen kansallisten säädösten ja määräysten mukaisesti, että oikeushenkilö tai luonnollinen henkilö täyttää edellytykset turvallisuusluokiteltuun tietoon pääsemiseksi ja sen käsittelemiseksi.

Artiklan 13 kohdan mukaan kolmannella osapuolella tarkoitetaan valtiota, järjestöä, oikeushenkilöä tai luonnollista henkilöä, joka ei ole sopimuksen osapuoli.

3 artikla. *Turvallisuusluokat.* 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 Kroatian turvallisuusluokituksen tasot vastaavat toisiaan. Korkein, ankarimpia tietoturvallisuustoimenpiteitä vaativa luokka on "ERITTÄIN SALAINEN/YTTERST HEMLIG" (VRLO TAJNO). Suomessa tähän luokkaan luetaan kuuluviksi tiedot, joiden luvaton ilmitulo voi aiheuttaa erittäin suurta vahinkoa maanpuolustukselle, turvallisuudelle, kansainvälisille suhteille tai muille yleisille eduille. Toiseksi korkein turvallisuusluokka on "SALAINEN/HEMLIG" (TAJNO). 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" (POVJERLJIVO), jolla tarkoitetaan Suomessa tietoja, joiden luvaton ilmitulo voi aiheuttaa vahinkoa maanpuolustukselle, turvallisuudelle, kansainvälisille suhteille tai muille yleisille eduille. Neljänteen asiakirjaluokkaan "KÄYTTÖ RAJOITETTU/BEGRÄNSAD TILLGÅNG" (OGRANIČENO) 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 vastaanottajan tulee varmistaa, ettei turvallisuusluokkaa muuteta eikä kumota ilman luovuttavan osapuolen antamaa kirjallista lupaa.

4 artikla. *Toimivaltaiset turvallisuusviranomaiset.* Artiklan 1 kohdassa on nimetty kummankin osapuolen kansalliset turvalli-

suusviranomaiset (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). Kroatiassa kansalliseksi turvallisuusviranomaiseksi on nimetty Office of the National Security Council.

Artiklan 2 kohdassa velvoitetaan osapuolet ilmoittamaan toisilleen kansallisten turvallisuusviranomaisten mahdollisista muutoksista. Kansalliset turvallisuusviranomaiset ilmoittavat toisilleen mahdollisista muista toimivaltaisista turvallisuusviranomaisista (Competent Security Authorities, CSA), ja näiden myöhemmistä muutoksista. Suomessa määrättyjä turvallisuusviranomaisia (Designated Security Authority, DSA) ovat kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 4 §:n mukaisesti puolustusministeriö, pääesikunta, Suojelupoliisi ja Viestintävirasto.

Artiklan 3 kohdassa velvoitetaan osapuolet ilmoittamaan toisilleen voimassa olevista kansallisista säädöksistä ja määräyksistä, joilla säännellään turvallisuusluokitellun tiedon suojaamista, sekä vaihtamaan pyynnöstä keskenään tietoja turvallisuusluokitellun tiedon suojaamisesta koskevista turvallisuusstandardeista, -menettelyistä ja –käytännöistä.

5 artikla. *Suojaustoimet ja pääsy turvallisuusluokiteltuun tietoon.* Artikla sisältää keskeiset vastavuoroista suojaamista koskevat velvoitteet.

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

Artiklan 2 kohdan mukaan luovuttavan osapuolen tulee ilmoittaa vastaanottavalle osapuolelle kirjallisesti luovutetun turvallisuusluokitellun tiedon turvallisuusluokan muutoksista, jotta vastaanottava osapuoli soveltaa sianmukaisia turvallisuustoimia.

Artiklan 3 kohta koskee henkilöstöturvallisuutta. Sen mukaan pääsy turvallisuusluokiteltuun tietoon sallitaan ainoastaan henkilöille, joilla on tiedonsaantitarve ja joista on tehty asianmukainen henkilöturvallisuusselvitys ja joille selvitetty heidän vastuunsa turvallisuusluokitellun tiedon suojaamisesta. Määräys on sopusoinnussa kansainvälisen tietoturvallisuusvelvoitteista annetun lain 6 §:n 3 momentin kanssa, jossa sallitaan tietoaineistoon pääsy vain niille henkilöille, jotka tarvitsevat tietoja tehtävänsä hoitamiseen. Kansainvälisen tietoturvallisuusvelvoitteen edellyttämä henkilöiden luotettavuuden varmistaminen toteutetaan Suomessa turvallisuusselvityksistä annetun lain sekä kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 11 §:n mukaisesti. Lakimuutosten tultua voimaan 1 päivänä tammikuuta 2015, henkilöturvallisuusselvitys tehdään siten kuin uudessa turvallisuusselvityslaissa säädetään ja henkilöturvallisuusselvitystodistus annetaan kansainvälisissä tietoturvallisuusvelvoitteista annetun lain mukaisesti (muutettu 11 §).

Artiklan 4 kohdan mukaan henkilöturvallisuusselvitystä ei edellytetä turvallisuusluokkaan KÄYTTÖ RAJOITETTU/BEGRÄNSAD TILLGÅNG/OGRANIČENO kuuluvan turvallisuusluokitellun tietoon pääsemiseksi.

Artiklan 5 kohdan mukaan kumpikin osapuoli tunnustaa toisen osapuolen antamat henkilö- ja yhteisöturvallisuusselvitykset.

Artiklan 6 kohdan mukaisesti toimivaltaiset turvallisuusviranomaiset avustavat toisiaan pyynnöstä, kansallisten säädöstensä ja määräystensä mukaisesti, sopimuksen soveltamiseksi tarvittavien selvitysmenettelyjen suorittamisessa. Avustaminen saattaa edellyttää tietojen vaihtoa, jolla on merkitystä suhteessa kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 17 §:ään. Sen mukaan Suomen viranomaisilla on oikeus antaa toiselle sopimuspuolelle kansainvälisen tietoturvallisuusvelvoitteen toteuttamiseksi välttämättömiä asiakirjoja ja tietoja sen estämättä, mitä asiakirjojen ja tietojen salassapidosta Suomen lainsäädännössä säädetään. Tämä ei kuitenkaan koske yksityisyyden suojan vuoksi salassa pidettäviksi säädettyjä tietoja. Uuden turvallisuusselvityslain mukaan henkilöturvallisuusselvitykseen voidaan sisällyttää tiet-

tyjä toisen valtion viranomaisen tietojärjestelmään talletettuja tietoja (25 ja 26 §).

Artiklan 7 kohdassa kansalliset turvallisuusviranomaiset velvoitetaan ilmoittamaan toisilleen viipymättä henkilö- ja yhteisöturvallisuusselvityksiin liittyvistä muutoksista.

Artiklan 8 kohdan mukaan vastaanottavan osapuolen kansallinen turvallisuusviranomainen antaa luovuttavan osapuolen turvallisuusviranomainen pyynnöstä kirjallisen vahvistuksen siitä, että henkilöllä on oikeus päästä turvallisuusluokiteltuun tietoon tai että yrityksellä on yhteisöturvallisuusselvitys.

Artiklan 9 a kohta kieltää turvallisuusluokitellun tiedon luovuttamisen kolmannelle osapuolelle ilman luovuttavan osapuolen kirjallista ennakkosuostumusta. Kohta velvoittaa osapuolet noudattamaan luovuttajan suostumuksen periaatetta.

Artiklan 9 b kohdan mukaan vastaanottavan osapuolen on merkittävä vastaanottamaansa turvallisuusluokiteltu tieto noudattaen 3 artiklan mukaista turvallisuusluokkien vastaavuutta. Velvoitetta vastaava säännös on kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 8 §:n 1 momentissa.

Artiklan 9 c kohdan mukaan turvallisuusluokiteltua tietoa saa käyttää ainoastaan siihen tarkoitukseen, jota varten se on annettu. Velvoitetta vastaava säännös on kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 6 §:n 2 momentissa.

Artiklan 10 kohdan mukaan jos muussa osapuolten välisessä sopimuksessa on ankarampia määräyksiä turvallisuusluokitellun tiedon vaihtamisesta tai suojaamisesta, sovelletaan näitä ankarampia määräyksiä.

6 artikla. *Turvallisuusluokitellun tiedon välittäminen.* Artikla sisältää määräykset menettelyistä siirrettäessä turvallisuusluokiteltuja tietoja osapuolten kesken.

Turvallisuusluokiteltu tieto välitetään 1 kohdan mukaan toimivaltaisen turvallisuusviranomaisten hyväksymiä kanavia käyttäen. Vastaanottava osapuoli vahvistaa turvallisuusluokkaan SALAINEN/HEMLIG/TAJNO ja sitä ylempään turvallisuusluokkaan kuuluvan tiedon vastaanottamisen.

Artiklan 2 kohdan mukaan turvallisuusluokiteltua tietoa välitetään 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.

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

Artiklan 1 kohdan mukaan turvallisuusluokkaan ERITTÄIN SALAINEN/YTTERSTHEMLIG/VRLO TAJNO kuuluvaa tietoa saa kääntää ja kopioida vain poikkeustapauksissa, luovuttavan osapuolen kirjallisella ennakkosuostumuksella.

Artiklan 2 kohdassa velvoitetaan tekemään turvallisuusluokitellun tiedon kopioihin alkuperäinen luokitusmerkintä. Tällainen kopio suojataan samalla tavalla kuin alkuperäinen tieto. Kopioita otetaan enintään viralliseen tarkoitukseen tarvittava määrä.

Artiklan 3 kohdassa velvoitetaan tekemään käännöksiin alkuperäinen luokitusmerkintä sekä lisäksi käännöskielinen merkintä siitä, että käännökset sisältävät luovuttavan osapuolen turvallisuusluokiteltua tietoa.

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.

8 artikla. *Turvallisuusluokitellun tiedon hävittäminen.* Artikla sisältää määräykset siitä, miten eri turvallisuusluokkiin kuuluvia aineistoja saa hävittää.

Artiklan 1 kohdan mukaan tieto hävitetään siten, että tiedon tuottaminen uudelleen kokonaan tai osittain saadaan estettyä

Artiklan 2 kohdan mukaan turvallisuusluokkaan ERITTÄIN SALAINEN/YTTERST HEMLIG/VRLO TAJNO kuuluvaa tietoa ei hävitetä vaan se palautetaan luovuttavalle osapuolelle.

Artiklan 3 kohdan mukaan luovuttava osapuoli voi nimenomaisesti kieltää turvallisuusluokitellun tiedon hävittämisen. Tällöin tieto palautetaan luovuttavalle osapuolelle.

Artiklan 4 kohdan mukaan kriisitilanteessa, jossa sopimuksen mukaisesti tuotetun tai vaihdetun turvallisuusluokitellun tiedon suojaaminen tai palauttaminen ei ole mahdollista, tieto hävitetään välittömästi. Vastaanottava osapuoli ilmoittaa tiedon hävittämisestä luovuttavan osapuolen kansalliselle 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 21 §:ssä säädetään asiakirjan arkistoimisesta ja hävittämisestä.

9 artikla. *Turvallisuusluokitellut sopimukset.* Artikla sisältää määräykset 2 artiklan 10 kohdassa tarkoitetun turvallisuusluokitellun sopimuksen tekemisestä jommankumman osapuolen alueella.

Artiklan 1 kohdan mukaan turvallisuusluokitellut sopimukset tehdään ja pannaan täytäntöön osapuolten kansallisten säädösten ja määräysten mukaisesti.

Artiklan 2 kohdan mukaan vastaanottavan osapuolen toimivaltainen turvallisuusviranomainen vahvistaa pyynnöstä, että ehdotetulla hankeosapuolella on annettu asianmukainen henkilö- tai yhteisöturvallisuusselvitys. Jos hankeosapuolella ei ole asianmukaista turvallisuusselvitystä, luovuttavan osapuolen kansallinen turvallisuusviranomainen voi pyytää, että vastaanottajan toimivaltainen turvallisuusviranomainen tekisi asianmukaisen turvallisuusselvityksen.

Artiklan 3 kohdan mukaan turvallisuusluokkaan KÄYTTÄ RAJOITETTU/BEGRÄNSAD TILLGÅNG/ OGRANIČENO kuuluvia turvallisuusluokiteltuja sopimuksia varten ei edellytetä yhteisöturvallisuusselvitystä.

Artiklan 4 kohta asettaa velvoitteen sisällyttää turvallisuusluokiteltuihin sopimuksiin asianmukaiset turvallisuusmääräykset, joissa luovuttava osapuoli määrittää vastaanottavalle osapuolelle luovutettavan turvallisuusluokitellun tiedon, tälle annetun turvallisuusluokan sekä hankeosapuolen velvoitteet turvallisuusluokitellun tiedon suojaamiseksi.

Artiklan 5 kohdassa on luettelo niistä velvoitteista, joita hankeosapuolella vähintään on turvallisuusluokitellun tiedon suojaamiseksi.

Turvallisuusluokiteltuja sopimuksia koskevat kansalliset säännökset sisältyvät kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 1 § 2 momenttiin (soveltaminen elinkeinonharjoittajaan), 2 §:n 2 kohtaan (erityissuojattava tietoaineisto), 7 §:ään (vaitiolovelvollisuus ja hyväksikäyttökielto) sekä 12 §:ään (yhteisöturvallisuusselvitys), 13 §:ään (sitoumus turvallisuustoimenpiteiden suorittamisesta) ja 14 §:ään (turvallisuustodistus). Kansainvälisten tietoturvallisuusvelvoitteista annetun lain muutosten tultua voimaan lain 12 §:ssä säädetään yritysturvallisuusselvitystodistuksesta, sen voimassaolosta ja peruuttamisesta ja lain 14 §:ssä todistusta koskevien tietojen merkitsemisestä turvallisuusselvitysrekisteriin. Lain sitoumusta koskeva 13 § kumotaan, mutta sitä vastaava säännös sisältyy uuteen turvallisuusselvityslakiin (40 §). Kansallinen sääntely vastaa sopimusvelvoitteen vaatimuksia. Velvoitteen täyttämiseksi tarpeellisesta suomalaisen viranomaisen tietojenanto-oikeudesta säädetään kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 17 §:ssä.

Artiklan 6 kohdan mukaan alihankkijoiden on noudatettava hankeosapuoliin sovellettavia turvallisuusmääräyksiä.

10 artikla. *Vierailut.* Artiklaa sovelletaan vierailuihin, joihin liittyy mahdollisuus saada turvallisuusluokiteltua tietoa. Artiklan 1 kohdan mukaan tällaiseen vierailuun vaaditaan isäntäosapuolen toimivaltaisen turvallisuusviranomaisen ennakolta antama lupa. Lupa myönnetään vierailevan osapuolen kansallisen turvallisuusviranomaisen esittämän vierailupyynnön perusteella.

Artiklan 2 kohdassa on luettelo tiedoista, jotka on sisällytettävä vierailulupapyyntöön.

Artiklan 3 kohta sisältää määräykset niistä menettelytavoista, joita noudatetaan järjestettäessä vierailuja. Kohdassa asetetun määrä-

ajan mukaan pyyntö tulee esittää vähintään kolme viikkoa etukäteen. Kiireellisissä tapauksissa toimivaltaiset turvallisuusviranomaiset voivat sopia lyhyemmästä ajankohdasta.

Artiklan 4 kohdan mukaan kumpikin osapuoli takaa vierailijoiden henkilötietojen suojaamisen kansallisten säädöstensä ja määräystensä mukaisesti.

11 artikla. *Tietoturvaloukkaus.* Artiklan 1 kohdassa kansalliset turvallisuusviranomaiset velvoitetaan ilmoittamaan viipymättä toisilleen tietoturvaloukkauksesta ja käynnistämään kansallisten säädöstensä ja määräystensä mukaisesti asianmukaisen menettelyn määrittääkseen loukkaukseen liittyvät tosiseikat. Menettelyn tuloksen toimitetaan luovuttavan osapuolen kansalliselle turvallisuusviranomaiselle.

Artiklan 2 kohdan mukaan jos tietoturvallisuusloukkaus on tapahtunut kolmannessa valtiossa, 1 kohdassa tarkoitetut toimet toteuttaa tiedot lähettänyt osapuoli.

Artiklan velvoitteisiin liittyvät säännökset sisältyvät kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 19 §:ään.

12 artikla. *Kustannukset.* Artiklan mukaan kumpikin osapuoli vastaa omista kustannuksistaan, jotka aiheutuvat sopimusta täytäntöön pantaessa ja sen täytäntöönpanoa valvoessa.

13 artikla. *Riitojen ratkaiseminen.* Artiklan mukaan kaikki sopimuksen tulkintaan tai soveltamiseen liittyvät osapuolten väliset riidat ratkaistaisiin yksinomaan osapuolten välisissä neuvotteluissa, eikä niitä saateta kansainvälisen tuomioistuimen tai kolmansien osapuolien ratkaistavaksi.

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

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 Kroatian välisen tietoturvallisuussopimuksen velvoitteiden toteuttamiseksi ei aineellista lainsäädäntöä ole tarpeen muuttaa, esitys sisältää vain ehdotuksen blankettilaiksi.

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

2 §. Sopimuksen muiden kuin lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta ja lain voimaantulosta säädettäisiin valtioneuvoston asetuksella. Laki on tarkoitus saattaa voimaan samanaikaisesti kuin sopimus tulee Suomen osalta voimaan.

3 Voimaantulo

Suomen ja Kroatian välisen sopimuksen 14 artiklan 1 kohdan mukaan sopimus tulee voimaan toiseksi seuraavan kuukauden ensimmäisenä päivänä sen jälkeen, kun on otettu vastaan jälkimmäinen kirjallinen ilmoitus, jolla osapuolet ilmoittavat toisilleen diplomaattiteitse, että niiden kansalliset sopimuksen voimaantulon edellyttämät oikeudelliset vaatimukset on täytetty.

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

4 Eduskunnan suostumuksen tarpeellisuus ja käsittelyjärjestys

4.1 Eduskunnan suostumuksen tarpeellisuus

Perustuslain 94 §:n 1 momentin mukaan eduskunta hyväksyy sellaiset valtiosopimukset ja muut kansainväliset velvoitteet, jotka sisältävät lainsäädännön alaan kuuluvia määräyksiä. Perustuslakivaliokunnan 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 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, turvallisuusluokitelluilla sopimuksilla, turvallisuusselvityksillä ja tietoturvaloukkauksella. Koska nämä määritelmät vaikuttavat joko suoraan tai välillisesti sopimuksen lainsäädännön alaan kuuluvien aineellisten määräysten tulkintaan ja soveltamiseen, ne edellyttävät eduskunnan hyväksymistä (PeVL 6/2001 vp).

Sopimuksen 3 artiklassa on määräykset turvallisuusluokitusmerkinnän tekemisestä ja turvallisuusluokkien vastaavuudesta. Yleisesti sovellettavat säännökset salassapito- ja luokitusmerkinnästä on säädetty julkisuuslain 25 §:ssä. Sen mukaan salassa pidettävään viranomaisen asiakirjaan on tehtävä merkintä asiakirjan salassa pitämisestä, kun tällainen asiakirja annetaan asianosaiselle ja kun asiakirja on pidettävä salassa toisen tai yleisen edun vuoksi. Muihin salaisiin asiakirjoihin tehtävä merkintä on harkinnanvarainen. Lisäksi kansainvälisistä tietoturvavelvoitteista annetun lain 8 §:ssä on säännökset turvallisuusluokan merkitsemisestä erityissuojattavaan tietoaineistoon. Sen mukaisesti erityissuojattavaan tietoaineistoon on julkisuuslain säännöksistä riippumatta tehtävä kansainvälisessä tietoturvallisuusvelvoitteessa määritelty merkintä sen osoittamiseksi, millaisia tietoturvallisuusvaatimuksia käsittelyssä on noudatettava. Määräys kuuluu lainsäädännön alaan.

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

Sopimuksen 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 9 a kohdassa on kyse sopimuksen ydinmääräyksestä, jonka perusteella Suomi voi suojata sopimuksen perusteella vaihdettua turvallisuusluokiteltua tietoa ilman julkisuuslaissa säädettyä vahinkoedellytysarviointia. Suomessa viranomaisten asiakirjojen julkisuus on pääsääntö. Jokaisella on perustuslain 12 §:n 2 momentin mukaan oikeus saada tieto viranomaisen julkisesta asiakirjasta. Tätä oikeutta voidaan rajoittaa välttämättömistä syistä vain lailla. Julkisuuslain säännöksistä poiketen kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 6 §:n 1 momentin mukaan erityissuojattava tietoaineisto on pidettävä salassa, jollei kansainvälisistä tietoturvallisuusvelvoitteesta muuta johdu. Sopimuksen 5 artiklan 3 kohdassa on ilmaistu myös turvallisuusluokiteltua tietoa saavia henkilöitä koskeva rajoitus. Artiklan 3 kohdassa määrätään myös osapuolten velvollisuudesta teettää asianmukainen turvallisuusselvitys henkilöistä, joilla on tai saattaa olla pääsy sopimuksessa tarkoitettuun turvallisuusluokiteltuun tietoon. Turvallisuusselvitysten laadinnassa on otettava huomioon perustuslain 10 §:n 1 momentissa säädetty yksityiselämän suoja ja velvollisuus säätää henkilötietojen suojasta lailla. Suomessa turvallisuusselvityksen kohteena olevista henkilöistä sekä selvityksessä sovellettavasta menettelystä on säädetty turvallisuusselvityksistä annetussa laissa (1 päivänä tammikuuta 2015 alkaen turvallisuusselvityslaissa). Määräys kuuluu siten lainsäädännön alaan ja edellyttää eduskunnan suostumusta voimaantullakseen. Sopimuksen 5 artiklan 9 c kohdan mukaan turvallisuusluokiteltua

tietoa saa käyttää ainoastaan siihen tarkoitukseen, jota varten se on annettu. Velvoitetta vastaava säännös on kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 6 §:n 2 momentissa. Kohdan määräys kuuluu näin ollen lainsäädännön alaan.

Sopimuksen 9 artiklassa on määräykset turvallisuusluokitelluista sopimuksista ja niitä tekevien yritysten turvallisuusselvityksistä. Yhteisöturvallisuusselvitystä koskevat säännökset sisältyvät kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 12 ja 13 §:ään. Vastaavat säännökset sisältyvät 1 päivänä tammikuuta 2015 voimaan tulevaan turvallisuusselvityslakiin. Samalla kansainvälistä tietoturvallisuusvelvoitteista annetun lain 11 ja 12 § muutetaan siten, että lain 11 § koskee henkilöturvallisuusselvitystodistusta, sen voimassaoloa ja peruuttamista ja 12 § yritysturvallisuusselvitystodistusta, sen voimassaoloa ja peruuttamista. Turvallisuusluokiteltuja sopimuksia ja yhteisöturvallisuustodistusta koskevat määräykset kuuluvat näin ollen lainsäädännön alaan.

Sopimuksen 11 artiklassa edellytetään, että kansalliset turvallisuusviranomaiset ilmoittavat viipymättä toisilleen tietoturvaloukkauksesta ja käynnistävät kansallisten säädöstensä ja määräystensä mukaisesti asianmukaisen menettelyn määrittääkseen loukkaukseen liittyvät tosiseikat. Menettelyn tuloksen toimitetaan luovuttavan osapuolen kansalliselle turvallisuusviranomaiselle. Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 19 §:ssä säädetään kansalliselle turvallisuusviranomaiselle kuuluvista velvoitteista sopimusmääräyksissä tarkoitetuissa tilanteissa. Artiklan määräykset kuuluvat näin ollen lainsäädännön alaan.

4.2 Käsittelyjärjestys

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

Suomen ja Kroatian 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 Kroatian tasavallan hallituksen välillä Zagrebissa 11 päivänä helmikuuta 2014 tehdyn sopimuksen.

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

Lakiehdotus

Laki

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

Eduskunnan päätöksen mukaisesti säädetään:

1 §

Turvallisuusluokitellun tiedon vastavuoroisesta suojaamisesta Suomen tasavallan hallituksen ja Kroatian tasavallan hallituksen välillä Zagrebissa 11 päivänä helmikuuta 2014 tehdyn sopimuksen lainsäädännön alaan kuuluvat määräykset ovat lakina voimassa sellaisina kuin Suomi on niihin sitoutunut.

2 §

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

Helsingissä 4 päivänä joulukuuta 2014

Pääministeri

ALEXANDER STUBB

Ulkoasiainneuvos *Maarit Jalava*

Sopimusteksti

SOPIMUS SUOMEN TASAVALLAN HALLITUKSEN JA KROATIAN TASAVALLAN HALLITUKSEN VÄLILLÄ TURVALLISUUSLUOKITELLUN TIEDON VASTAVUOROISESTA SUOJAAMISESTA

Suomen tasavallan hallitus ja Kroatian tasavallan hallitus (jäljempänä "osapuolet"), jotka

ottavat huomioon, että osapuolet toimivat yhteistyössä muun muassa, mutta eivät yksinomaan, ulko-, puolustus-, turvallisuus- ja poliisiasioissa sekä tiede-, elinkeino- ja teknologia-asioissa,

ymmärtävät, että hyvä yhteistyö saattaa edellyttää turvallisuusluokitellun tiedon vaihtamista osapuolten kesken,

haluavat luoda säännöstön, jolla säännellään sellaisen turvallisuusluokitellun tiedon vastavuoroista suojaamista, jota tuotetaan tai vaihdetaan osapuolten kesken tai niiden lainkäyttövaltaan kuuluvien julkis- tai yksityisoikeudellisten oikeushenkilöiden tai luonnollisten henkilöiden kesken,

ovat sopineet seuraavasta:

1 artikla

Tavoite

Tämän sopimuksen tavoitteena on varmistaa sellaisen turvallisuusluokitellun tiedon suojaaminen, jota tuotetaan tai vaihdetaan yleisesti osapuolten kesken.

2 artikla

Määritelmät

Tässä sopimuksessa

(1) **"turvallisuusluokiteltu tieto"** tarkoittaa missä tahansa muodossa olevaa tietoa, jo-

AGREEMENT BETWEEN THE GOVERNMENT OF THE REPUBLIC OF FINLAND AND THE GOVERNMENT OF THE REPUBLIC OF CROATIA ON MUTUAL PROTECTION OF CLASSIFIED INFORMATION

The Government of the Republic of Finland and the Government of the Republic of Croatia (hereinafter referred to as “the Parties”),

Considering that the Parties co-operate in matters such as, but not limited to, foreign affairs, defence, security, police, and science, industry and technology,

Realizing that good co-operation may require the exchange of Classified Information between the Parties,

Desiring to establish a set of rules regulating the mutual protection of Classified Information generated or exchanged between the Parties, or public or private legal entities or individuals under the jurisdiction of the Parties,

Have agreed as follows:

Article 1

Objective

The objective of this Agreement is to ensure the protection of Classified Information that is commonly generated or exchanged between the Parties.

Article 2

Definitions

For the purposes of this Agreement:

(1) **“Classified Information”** means any information, irrespective of form, which re-

ka on suojattava tietoturvaloukkaukselta ja on luokiteltu luovuttavan osapuolen kansallisten säädösten ja määräysten mukaisesti;

(2) **"tiedonsaantitarve"** tarkoittaa tarvetta päästä turvallisuusluokiteltuun tietoon tietyssä virallisessa asemassa toimittaessa ja tietyn tehtävän suorittamiseksi;

(3) **"tietoturvaloukkaus"** tarkoittaa missä tahansa muodossa tapahtuvaa turvallisuusluokitellun tiedon luvatonta ilmaisemista tai muuttamista, väärinkäyttöä, vahingoittamista tai hävittämistä taikka muuta sellaista tekoa tai laiminlyöntiä, jonka johdosta tieto voi menettää salassapitonsa, eheytensä tai käytettävyytensä;

(4) **"turvallisuusluokka"** tarkoittaa luokkaa, joka kansallisten säädösten ja määräysten mukaisesti ilmaisee niiden rajoitusten tason, joilla osapuolet rajoittavat pääsyä turvallisuusluokiteltuun tietoon, sekä osapuolten tälle tiedolle antaman suojan vähimmäistason;

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

(6) **"vastaanottava osapuoli"** tarkoittaa osapuolta sekä sen lainkäyttövaltaan kuuluvaa julkis- tai yksityisoikeudellista oikeushenkilöä tai luonnollista henkilöä, jolle luovuttavan osapuolen turvallisuusluokiteltu tieto välitetään;

(7) **"kansallinen turvallisuusviranomainen"** tarkoittaa kansallista viranomaista, joka vastaa tämän sopimuksen täytäntöönpanosta ja sen valvonnasta;

(8) **"toimivaltainen turvallisuusviranomainen"** tarkoittaa kansallista turvallisuusviranomaista, määrättyä turvallisuusviranomaista tai kansallista tietoturvaviranomaista tai muuta sellaista kansallista viranomaista, joka panee täytäntöön tätä sopimusta kansallisten säädösten ja määräysten mukaisesti;

(9) **"hankeosapuoli"** tarkoittaa luonnollista henkilöä tai oikeushenkilöä, jolla on oikeudellinen kelpoisuus tehdä sopimuksia;

(10) **"turvallisuusluokiteltu sopimus"** tarkoittaa kahden tai useamman hankeosapuolen välistä sopimusta, johon sisältyy pääsy turvallisuusluokiteltuun tietoon tai jonka täytäntöönpano edellyttää tätä;

quires protection against Security Breach and has been classified in accordance with national laws and regulations of the Originating Party;

(2) **"Need-to-Know"** means the necessity to have access to Classified Information in the scope of a given official position and for the performance of a specific task;

(3) **"Security Breach"** means any form of unauthorized disclosure or alteration, misuse, damage or destruction of Classified Information, as well as any other action or inaction which may result in loss of its confidentiality, integrity or availability;

(4) **"Security Classification Level"** means a category which, in accordance with national laws and regulations, characterises the level of restriction of access to Classified Information and the minimum level of its protection by the Parties;

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

(6) **"Receiving Party"** means the Party, as well as any public or private legal entity or individual under its jurisdiction, to which Classified Information of the Originating Party is transmitted;

(7) **"National Security Authority"** means the national authority responsible for the implementation and supervision of this Agreement;

(8) **"Competent Security Authority"** means the National Security Authority, Designated Security Authority or National Communications Security Authority or another national authority which, in accordance with national laws and regulations, implements this Agreement;

(9) **"Contractor"** means an individual or a legal entity possessing the legal capacity to conclude contracts;

(10) **"Classified Contract"** means an agreement between two or more Contractors which involves or the execution of which requires access to Classified Information;

(11) **"henkilöturvallisuusselvitys"** tarkoittaa toimivaltaisen turvallisuusviranomaisen kansallisten säädösten ja määräysten mukaisesti tekemää arviota, jonka mukaan luonnolliselle henkilölle voidaan sallia pääsy turvallisuusluokiteltuun tietoon;

(12) **"yhteisöturvallisuusselvitys"** tarkoittaa toimivaltaisen turvallisuusviranomaisen tekemää arviota, jolla vahvistetaan kyseisen osapuolen kansallisten säädösten ja määräysten mukaisesti, että oikeushenkilö tai luonnollinen henkilö täyttää edellytykset turvallisuusluokiteltuun tietoon pääsemiseksi ja sen käsittelemiseksi;

(13) **"kolmas osapuoli"** tarkoittaa valtiota, järjestöä, oikeushenkilöä tai luonnollista henkilöä, joka ei ole tämän sopimuksen osapuoli.

(11) **"Personnel Security Clearance"** means determination by the Competent Security Authority confirming, in accordance with its national laws and regulations, that an individual is eligible to have access to Classified Information;

(12) **"Facility Security Clearance**" means determination by the Competent Security Authority confirming, in accordance with its national laws and regulations, that a legal entity or individual meets the conditions for access to and handling of Classified Information;

(13) **"Third Party"** means any state, organization, legal entity or individual which is not a party to this Agreement.

3 artikla

Turvallisuusluokat

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

2. Osapuolet sopivat, että seuraavat turvallisuusluokat vastaavat toisiaan:

Article 3

Security Classification Levels

1. Any Classified Information provided under this Agreement shall be marked with the appropriate Security Classification Level in accordance with national laws and regulations of the Parties.

2. The Parties agree that the following Security Classification Levels are equivalent to each other:

Suomen tasavalta	Englanninkielinen vastine	Kroatian tasavalta
ERITTÄIN SALAINEN tai YTTERST HEMLIG	TOP SECRET	VRLO TAJNO
SALAINEN tai HEMLIG	SECRET	TAJNO
LUOTTAMUKSELLINEN tai KONFIDENTIELL	CONFIDENTIAL	POVJERLJIVO
KÄYTTÖ RAJOITETTU tai BEGRÄNSAD TILLGÅNG	RESTRICTED	OGRANIČENO

For the Republic of Finland	Equivalent in English	For the Republic of Croatia
ERITTÄIN SALAINEN or YTTERST HEMLIG	TOP SECRET	VRLO TAJNO

SALAINEN or HEMLIG	SECRET	TAJNO
LUOTTAMUKSELLINEN or KONFIDENTIELL	CONFIDENTIAL	POVJERLJIVO
KÄYTTÖ RAJOITETTU or BEGRÄNSAD TILLGÅNG	RESTRICTED	OGRANIČENO

3. Vastaanottava osapuoli varmistaa, ettei tiedon turvallisuusluokituksia muuteta eikä kumota, ellei luovuttava osapuoli anna siihen kirjallista lupaa.

4 artikla

Toimivaltaiset turvallisuusviranomaiset

1. Osapuolten kansalliset turvallisuusviranomaiset ovat
Suomen tasavallassa
- ulkoasiainministeriö;
Kroatian tasavallassa
- Office of the National Security Council.
2. Osapuolet ilmoittavat toisilleen diplomaattiteitse kansallisten turvallisuusviranomaisten mahdollisista muutoksista. Kansalliset turvallisuusviranomaiset ilmoittavat toisilleen mahdollisista muista toimivaltaisista turvallisuusviranomaisista ja näiden myöhemmistä muutoksista.
3. Kansalliset turvallisuusviranomaiset ilmoittavat toisilleen voimassa olevista kansallisista säädöksistä ja määräyksistä, joilla säännellään turvallisuusluokitellun tiedon suojaamista, sekä vaihtavat pyynnöstä keskenään tietoja turvallisuusluokitellun tiedon suojaamista koskevista turvallisuusstandardeista, -menettelyistä ja -käytännöistä.

5 artikla

Suojaustoimet ja pääsy turvallisuusluokiteltuun tietoon

1. Osapuolet toteuttavat kansallisten säädöstensä ja määräystensä mukaisesti kaikki asianmukaiset toimet tämän sopimuksen mukaisesti tuotettavan tai vaihdettavan turvallisuusluokitellun tiedon suojaamiseksi. Tällaiselle turvallisuusluokitellulle tiedolle varmistetaan samantasoinen suoja kuin vastaavaan

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

Article 4

Competent Security Authorities

1. The National Security Authorities of the Parties are:
For the Republic of Finland:
- Ministry for Foreign Affairs;
For the Republic of Croatia:
- Office of the National Security Council.
2. The Parties shall inform each other through diplomatic channels of any changes of the National Security Authorities. The National Security Authorities shall inform each other of any other Competent Security Authorities and any subsequent changes of these authorities.
3. The National Security Authorities shall inform each other of the national laws and regulations in force regulating the protection of Classified Information and shall, on request, exchange information about the security standards, procedures and practices for the protection of Classified Information.

Article 5

Protection Measures and Access to Classified Information

1. In accordance with their national laws and regulations, the Parties shall take all appropriate measures for the protection of Classified Information generated or exchanged under this Agreement. The same level of protection shall be ensured for such Classified Information as is provided to the national

tämän sopimuksen 3 artiklassa määriteltyyn turvallisuusluokkaan kuuluvalle kansalliselle turvallisuusluokitellulle tiedolle.

2. Luovuttava osapuoli ilmoittaa vastaanottavalle osapuolelle kirjallisesti luovutetun turvallisuusluokitellun tiedon turvallisuusluokan muutoksista, jotta vastaanottava osapuoli soveltaa asianmukaisia turvallisuustoimia.

3. Pääsy turvallisuusluokiteltuun tietoon sallitaan ainoastaan sellaisille luonnollisille henkilöille, joilla on tiedonsaantitarve ja joille on annettu asianmukainen henkilöturvallisuusselvitys kyseisen osapuolen kansallisten säädösten ja määräysten mukaisesti sekä selvitetty heidän vastuunsa turvallisuusluokitellun tiedon suojaamisesta.

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

5. Tätä sopimusta sovellettaessa kumpikin osapuoli tunnustaa toisen osapuolen antamat henkilö- ja yhteisöturvallisuusselvitykset.

6. Toimivaltaiset turvallisuusviranomaiset avustavat toisiaan pyynnöstä, kansallisten säädöstensä ja määräystensä mukaisesti, tämän sopimuksen soveltamiseksi tarvittavien selvitysmenettelyjen suorittamisessa.

7. Tätä sopimusta sovellettaessa kansalliset turvallisuusviranomaiset ilmoittavat toisilleen viipymättä henkilö- ja yhteisöturvallisuusselvityksiin liittyvistä muutoksista, erityisesti turvallisuusluokkien kumoamisesta tai muuttamisesta.

8. Luovuttavan osapuolen kansallisen turvallisuusviranomaisen pyynnöstä vastaanottavan osapuolen kansallinen turvallisuusviranomainen antaa kirjallisen vahvistuksen siitä, että luonnollisella henkilöllä on oikeus päästä turvallisuusluokiteltuun tietoon tai että oikeushenkilölle on annettu yhteisöturvallisuusselvitys.

9. Vastaanottava osapuoli

a) välittää turvallisuusluokiteltua tietoa kolmannelle osapuolelle ainoastaan luovuttavan osapuolen kirjallisella ennakkosuostumuksella;

Classified Information of the equivalent Security Classification Level, as defined in Article 3 of this Agreement.

2. The Originating Party shall inform the Receiving Party in writing about any change of the Security Classification Level of the released Classified Information, in order that the latter apply the appropriate security measures.

3. Access to Classified Information shall only be granted to individuals who have a Need-to-Know, who have been issued an appropriate Personnel Security Clearance in accordance with the national laws and regulations and who have been 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 or BEGRÄNSAD TILLGÅNG / OGRANIČENO level.

5. Within the scope of this Agreement, each Party shall recognize the Personnel and Facility Security Clearances issued by the other Party.

6. The Competent Security Authorities shall assist each other upon request and in accordance with their national laws and regulations in carrying out vetting procedures necessary for the application of this Agreement.

7. Within the scope of this Agreement, the National Security Authorities shall inform each other without delay about any alteration with regard to Personnel and Facility Security Clearances, in particular about the revocation or the alteration of Security Classification Levels.

8. Upon request of the National Security Authority of the Originating Party, the National Security Authority of the Receiving Party shall issue a written confirmation that an individual has the right to access Classified Information or a legal entity has been issued a Facility Security Clearance.

9. The Receiving Party shall:

a) submit Classified Information to a Third Party only upon prior written consent of the Originating Party;

b) merkitsee vastaanottamansa turvallisuusluokitellun tiedon noudattaen 3 artiklan mukaista turvallisuusluokkien vastaavuutta;

c) käyttää turvallisuusluokiteltua tietoa ainoastaan niihin tarkoituksiin, joita varten se on luovutettu.

10. Jos muussa osapuolten välisessä sopimuksessa on ankarampia määräyksiä turvallisuusluokitellun tiedon vaihtamisesta tai suojaamisesta, sovelletaan näitä ankarampia määräyksiä.

b) mark the received Classified Information in accordance with the Security Classification Level equivalence set forth in Article 3;

c) use Classified Information only for the purposes that it has been provided for.

10. If any other agreement concluded between the Parties contains stricter regulations regarding the exchange or protection of Classified Information, these stricter regulations shall apply.

6 artikla

Turvallisuusluokitellun tiedon välittäminen

1. Turvallisuusluokiteltu tieto välitetään käyttäen toimivaltaisten turvallisuusviranomaisten keskenään hyväksymiä kanavia. Vastaanottava osapuoli vahvistaa turvallisuusluokkaan SALAINEN tai HEMLIG / TAJNO ja sitä ylempään turvallisuusluokkaan kuuluvan tiedon vastaanottamisen. Muun turvallisuusluokitellun tiedon vastaanottaminen vahvistetaan pyynnöstä.

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

Article 6

Transmission of Classified Information

1. Classified Information shall be transmitted through channels mutually approved by the Competent Security Authorities. The Receiving Party shall confirm the receipt of Classified Information at the levels SALAINEN or HEMLIG / TAJNO and above. The receipt of other Classified Information shall be confirmed on request.

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

7 artikla

Turvallisuusluokitellun tiedon kopiointi ja kääntäminen

1. Turvallisuusluokkaan ERITTÄIN SALAINEN tai YTTERST HEMLIG / VRLO TAJNO kuuluvaa tietoa käännetään tai kopioidaan ainoastaan poikkeustapauksissa, luovuttavan osapuolen kirjallisella ennakkosuostumuksella.

2. Kaikkiin turvallisuusluokitellun tiedon kopioihin merkitään alkuperäinen luokitusmerkintä. Tällainen kopioitu tieto suojataan samalla tavoin kuin alkuperäinen tieto. Kopioita otetaan enintään virallisiin tarkoituksiin tarvittava määrä.

3. Turvallisuusluokitellun tiedon käännökseen tehdään alkuperäinen luokitusmerkintä sekä lisäksi käännöskielinen huomautus siitä, että käännös sisältää luovuttavan osapuolen

Article 7

Reproduction and Translation of Classified Information

1. Information classified at the ERITTÄIN SALAINEN or YTTERST HEMLIG / VRLO TAJNO level shall be translated or reproduced only in exceptional cases upon prior written consent of the Originating Party.

2. All copies of Classified Information shall be marked with the original classification marking. Such reproduced information shall be protected in the same way as the original information. The number of copies shall be limited to that required for official purposes.

3. Any translation of Classified Information shall be marked with the original classification marking and bear an additional note in the language of translation that the transla-

turvallisuusluokiteltua tietoa.

8 artikla

Turvallisuusluokitellun tiedon hävittäminen

1. Jotta turvallisuusluokitellun tiedon tuottaminen uudelleen kokonaan tai osittain saadaan estetyksi, tieto hävitetään.
2. Turvallisuusluokkaan ERITTÄIN SALAINEN tai YTTERST HEMLIG / VRLO TAJNO kuuluvaa tietoa ei hävitetä. Se palautetaan luovuttavalle osapuolelle.
3. Luovuttava osapuoli voi lisämerkinnän avulla tai myöhemmällä kirjallisella ilmoituksella nimenomaisesti kieltää turvallisuusluokitellun tiedon hävittämisen. Jos turvallisuusluokitellun tiedon hävittäminen kielletään, tieto palautetaan luovuttavalle osapuolelle.
4. Kriisitilanteessa, joka estää tämän sopimuksen mukaisesti tuotetun tai vaihdetun turvallisuusluokitellun tiedon suojaamisen tai palauttamisen, tieto hävitetään välittömästi. Vastaanottava osapuoli ilmoittaa tiedon hävittämisestä luovuttavan osapuolen kansalliselle turvallisuusviranomaiselle mahdollisimman pian.

9 artikla

Turvallisuusluokitellut sopimukset

1. Turvallisuusluokitellut sopimukset tehdään ja pannaan täytäntöön kummankin osapuolen kansallisten säädösten ja määräysten mukaisesti.
2. Vastaanottavan osapuolen kansallinen turvallisuusviranomainen vahvistaa pyynnöstä, että ehdotetulle hankeosapuolelle on annettu asianmukainen henkilö- tai yhteisöturvallisuusselvitys. Jos ehdotetulla hankeosapuolella ei ole asianmukaista turvallisuusselvitystä, luovuttavan osapuolen kansallinen turvallisuusviranomainen voi pyytää vastaanottavan osapuolen kansallista turvallisuusviranomaista antamaan asianmukaisen turvallisuusselvityksen.
3. Turvallisuusluokkaan KÄYTTÖ RAJOITETTU tai BEGRÄNSAD TILLGÅNG / OGRANIČENO kuuluvia turvallisuusluokitteltua tietoa.

tion contains Classified Information of the Originating Party.

Article 8

Destruction of Classified Information

1. Classified Information shall be destroyed insofar as to prevent its reconstruction in whole or in part.
2. Classified information at the ERITTÄIN SALAINEN or YTTERST HEMLIG / VRLO TAJNO level shall not be destroyed. It shall be returned to the Originating Party.
3. The Originating Party may, by additional marking or subsequent written notice, expressly prohibit the destruction of Classified Information. If the destruction of Classified Information is prohibited, it shall be returned to the Originating Party.

4. In case of a crisis situation which makes it impossible to protect or return Classified Information generated or exchanged under this Agreement the Classified Information shall be destroyed immediately. The Receiving Party shall notify the National Security Authority of the Originating Party about this destruction as soon as possible.

Article 9

Classified Contracts

1. Classified Contracts shall be concluded and implemented in accordance with national laws and regulations of each Party.

2. Upon request the National Security Authority of the Receiving Party shall confirm that a proposed Contractor has been issued an appropriate Personnel or Facility Security Clearance. If the proposed Contractor does not hold an appropriate security clearance, the National Security Authority of the Originating Party may request the National Security Authority of the Receiving Party to issue the appropriate security clearance.

3. A Facility Security Clearance is not required for Classified Contracts at the KÄYTTÖ RAJOITETTU or BEGRÄNSAD

teltuja sopimuksia varten ei edellytetä yhteisöturvallisuusselvitystä.

4. Kuhunkin turvallisuusluokiteltuun sopimukseen ja alihankintasopimukseen on sisällytettävä turvallisuusmääräykset, joissa luovuttava osapuoli määrittää vastaanottavalle osapuolelle luovutettavan turvallisuusluokitellun tiedon, tälle annetun turvallisuusluokan sekä hankeosapuolen velvoitteet turvallisuusluokitellun tiedon suojaamiseksi.

5. Hankeosapuolella on turvallisuusluokitellun tiedon suojaamiseksi vähintään seuraavat velvoitteet:

a) sallia pääsy turvallisuusluokiteltuun tietoon kyseisen osapuolen kansallisten säädösten ja määräysten sekä tämän sopimuksen mukaisesti;

b) välittää turvallisuusluokiteltu tieto tässä sopimuksessa määritettyjä keinoja käyttäen;

c) ilmoittaa mahdollisista turvallisuusluokiteltuun tietoon liittyvistä muutoksista;

d) käyttää turvallisuusluokiteltuun sopimukseen liittyvää turvallisuusluokiteltua tietoa ainoastaan sopimuksen aiheeseen liittyviin tarkoituksiin;

e) noudattaa tarkasti tämän sopimuksen määräyksiä, jotka liittyvät turvallisuusluokitellun tiedon käsittelymenettelyihin:

f) ilmoittaa hankeosapuolen kansalliselle turvallisuusviranomaiselle mahdollisesta turvallisuusluokiteltuun sopimukseen liittyvästä tietoturvaloukkauksesta;

g) luovuttaa turvallisuusluokiteltuun sopimukseen liittyvää turvallisuusluokiteltua tietoa kolmannelle osapuolelle ainoastaan luovuttavan osapuolen kirjallisella ennakkosuostumuksella.

6. Turvallisuusluokiteltujen sopimusten täytäntöönpanoon osallistuvien alihankkijoiden on tapauksen mukaan noudatettava hankeosapuoliin sovellettavia turvallisuusmääräyksiä.

TILLGÅNG / OGRANIČENO level.

4. Each Classified Contract or sub-contract shall include security provisions by which the Originating Party shall specify the Classified Information to be released to the Receiving Party, the Security Classification Level assigned to that information, and the Contractor's obligations to protect the Classified Information.

5. The Contractor's obligations to protect Classified Information shall include, at least, the following:

a) to grant access to the Classified Information in accordance with the national laws and regulations and this Agreement;

b) to transmit the Classified Information by the means specified in this Agreement;

c) to communicate any changes that may arise in respect of the Classified Information;

d) to use the Classified Information under the Classified Contract only for the purposes related to the subject of the contract;

e) to adhere strictly to the provisions of this Agreement related to the procedures for handling Classified Information;

f) to notify the Contractor's National Security Authority of any Security Breach related to the Classified Contract;

g) to release the Classified Information related to the Classified Contract to any Third Party only upon prior written consent of the Originating Party.

6. Sub-contractors engaged in Classified Contracts shall, as appropriate, comply with the security provisions applied to the Contractors.

10 artikla

Vierailut

1. Vierailut, joihin liittyy pääsy turvallisuusluokiteltuun tietoon, edellyttävät isäntäosapuolen kansallisen turvallisuusviranomaisen ennakolta antamaa lupaa. Lupa myönnetään vierailevan osapuolen kansallisen turval-

Article 10

Visits

1. Visits entailing access to Classified Information are subject to prior permission by the National Security Authority of the host Party. The permission shall be granted on the basis of a visit request by the National Secu-

lisuusviranomaisen esittämän vierailupyynnön perusteella.

2. Tämän artiklan 1 kohdassa tarkoitetun pyynnön on sisällettävä

a) vierailijan etu- ja sukunimi, syntymäaika ja -paikka sekä kansallisuus;

b) vierailijan passin tai muun henkilötodistuksen numero;

c) vierailijan asema ja hänen edustamansa organisaation nimi;

d) vierailijan henkilöturvallisuusselvityksen taso;

e) vierailun tarkoitus ja ehdotettu työohjelma, mukaan lukien vierailuun liittyvän turvallisuusluokitellun tiedon korkein turvallisuusluokka, sekä suunniteltu vierailuajankohta;

f) vierailupyynnössä tarkoitettujen organisaatioiden ja toimipaikkojen nimet;

g) vierailujen määrä ja kesto;

h) mahdolliset muut tiedot, joista kansalliset turvallisuusviranomaiset sopivat keskenään.

3. Tämän artiklan 1 kohdassa tarkoitettu pyyntö esitetään vähintään kolme viikkoa etukäteen. Kiireellisissä tapauksissa kansalliset turvallisuusviranomaiset voivat sopia lyhyemmästä ajasta.

4. Kumpikin osapuoli takaa vierailijoiden henkilötietojen suojaamisen kansallisten säädöstensä ja määräystensä mukaisesti.

11 artikla

Tietoturvaloukkaus

1. Tietoturvaloukkauksen tapahduttua sen osapuolen kansallinen turvallisuusviranomainen, jonka alueella loukkaus on tehty, ilmoittaa loukkauksesta viipymättä luovuttavan osapuolen kansalliselle turvallisuusviranomaiselle ja käynnistää kansallisten säädöstensä ja määräystensä mukaisesti asianmukaisen menettelyn määrittääkseen loukkaukseen liittyvät tosiseikat. Menettelyn tulokset toimitetaan luovuttavan osapuolen kansalliselle turvallisuusviranomaiselle.

2. Kun tietoturvaloukkaus on tehty kolmannessa valtiossa, turvallisuusluokitellut tiedot lähettäneen osapuolen kansallinen turvallisuusviranomainen toteuttaa viipymättä tämän artiklan 1 kohdassa tarkoitetut toimet.

rity Authority of the visiting Party.

2. The request referred to in paragraph 1 of this Article shall contain:

a) the visitor's name and surname, date and place of birth, and nationality;

b) the passport number or another identification card number of the visitor;

c) the position of the visitor and the name of the organization represented;

d) the level of the Personnel Security Clearance of the visitor;

e) the purpose, proposed working programme, including the highest level of Classified Information involved, and planned date of the visit;

f) the names of the organizations and facilities requested to be visited;

g) the number of visits and the period required;

h) any other data, agreed upon by the National Security Authorities.

3. The request referred to in paragraph 1 of this Article shall be submitted at least 3 weeks in advance. In urgent cases the National Security Authorities may agree on a shorter period.

4. Each Party shall guarantee the protection of the personal data of the visitors in accordance with its national laws and regulations.

Article 11

Security Breach

1. In case of a Security Breach, the National Security Authority of the Party where the breach has occurred shall, without delay, inform the National Security Authority of the Originating Party about the breach and, in accordance with national laws and regulations, initiate appropriate proceedings in order to determine the circumstances of the Security Breach. The results of the proceedings shall be forwarded to the National Security Authority of the Originating Party.

2. When the Security Breach has occurred in a third state, the National Security Authority of the sending Party shall take the actions referred to in paragraph 1 of this Article without delay.

12 artikla

Kustannukset

Osapuolet vastaavat omista kustannuksistaan, jotka aiheutuvat tätä sopimusta täytäntöön pantaessa ja sen täytäntöönpanoa valvottaessa.

Article 12

Expenses

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

13 artikla

Riitojen ratkaiseminen

Kaikki tämän sopimuksen tulkintaa tai soveltamista koskevat riidat ratkaistaan osapuolten välisillä keskusteluilla ja neuvotteluilla, eikä niitä saateta kansainvälisten tuomioistuinten tai kolmansien osapuolten ratkaistaviksi.

Article 13

Settlement of Disputes

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

14 artikla

Loppumääräykset

1. Tämä sopimus tulee voimaan toiseksi seuraavan kuukauden ensimmäisenä päivänä sen jälkeen, kun on otettu vastaan jälkimmäinen kirjallinen ilmoitus, jolla osapuolet ilmoittavat toisilleen diplomaattiteitse, että niiden kansalliset sopimuksen voimaantulon edellyttämät oikeudelliset vaatimukset on täytetty.

2. Tätä sopimusta voidaan muuttaa osapuolten keskinäisellä kirjallisella suostumuksella. Muutokset tulevat voimaan tämän artiklan 1 kohdan mukaisesti.

3. Tämä sopimus tehdään toistaiseksi. Osapuoli voi irtisanoa tämän sopimuksen ilmoittamalla asiasta toiselle osapuolelle kirjallisesti diplomaattiteitse. Tällöin tämä sopimus lakkaa olemasta voimassa kuuden kuukauden kuluttua siitä päivästä, jona toinen osapuoli on vastaanottanut irtisanomisilmoituksen.

4. Jos tämä sopimus lakkaa olemasta voimassa, kaikkea sopimuksen mukaisesti vaihdettua turvallisuusluokiteltua tietoa suojataan edelleen sopimuksen määräyksiä noudattaen, ja pyynnöstä tämä tieto palautetaan luovuttavalle osapuolelle.

Article 14

Final Provisions

1. This Agreement shall enter into force on the first day of the second month following the receipt of the last written notification by which the Parties have informed each other, through diplomatic channels, that their internal legal requirements necessary for the entry into force of the Agreement have been fulfilled.

2. This Agreement may be amended by mutual written consent of the Parties. The amendments shall enter into force in accordance with the provision of paragraph 1 of this Article.

3. This Agreement is concluded for an indefinite period of time. Either Party may denounce this Agreement by giving the other Party written notice through diplomatic channels. In that case, this Agreement shall terminate six months from the date on which the other Party has received the denunciation notice.

4. In case of termination of this Agreement, all Classified Information exchanged pursuant to this Agreement shall continue to be protected in accordance with the provisions set forth herein and, upon request, returned to the Originating Party.

Tehty Zagrebissa 11 päivänä helmikuuta 2014 kahtena suomen-, kroatian- ja englanninkielisenä alkuperäiskappaleena, jonka kaikki tekstit ovat yhtä todistusvoimaiset. Jos syntyy tulkintaeroja, englanninkielinen teksti on ratkaiseva.

Done at Zagreb on 11th February in two originals, each in the Finnish, Croatian and English languages, all texts being equally authentic. In case of any divergence of interpretation, the English text shall prevail.

Suomen tasavallan hallituksen puolesta

Timo Rajakangas
suurlähettiläs

For the Government of the Republic of Finland

Timo Rajakangas
Ambassador

Kroatian tasavallan hallituksen puolesta

Ivica Panenic
Kansallisen turvallisuusneuvoston toimiston päällikkö

For the Government of the Republic of Croatia Kroatian tasavallan hallituksen puolesta

Ivica Panenic
Head of the Office of the National Security Council