HE 139/2012 vp

Hallituksen esitys eduskunnalle Suomen ja Pohjois-Atlantin liiton kesken vaihdettavan turvallisuusluokitellun tiedon suojaamisesta tehdyn hallinnollisen järjestelyn hyväksymisestä sekä laiksi järjestelyn ja Pohjois-Atlantin liiton kanssa tehdyn tietoturvallisuussopimuksen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta

ESITYKSEN PÄÄASIALLINEN SISÄLTÖ

Esityksessä ehdotetaan, että eduskunta hyväksyisi Suomen ja Pohjois-Atlantin liiton kesken vaihdettavan turvallisuusluokitellun tiedon suojaamisesta tehdyn hallinnollisen järjestelyn sekä lain järjestelyn ja Pohjois-Atlantin liiton kanssa tehdyn tietoturvallisuussopimuksen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta.

Järjestelyn tarkoituksena on ajantasaistaa Suomen ja Pohjois-Atlantin liiton välillä vuonna 1994 tehty tietoturvallisuussopimus siten, että turvallisuusluokiteltujen tietojen suojaamisessa otettaisiin huomioon kansainvälisistä tietoturvallisuusvelvoitteista annetun lain säännökset sekä nykyiset turvallisuusmääräykset. Samassa yhteydessä on tarkoitus saattaa voimaan Suomen ja Pohjois-Atlantin liiton välillä vuonna 1994 tehty tietoturvallisuussopimus.

Järjestely tulee voimaan päivänä, jonka Suomi ilmoittaa Pohjois-Atlantin liitolle sen jälkeen, kun Suomen kansalliset hyväksymistoimet on suoritettu. Laki on tarkoitettu tulemaan voimaan valtioneuvoston asetuksella säädettävänä ajankohtana samaan aikaan kuin järjestely tulee Suomen osalta voimaan.

296160

SISÄLLYS

YLEISPERUSTELUT

1 Johdanto

Pohjois-Atlantin liiton (Nato) turvallisuustoimisto (NATO Office of Security, NOS) esitti Suomelle turvallisuusluokitellun tiedon suojaamista koskevan sopimuksen, jäljempänä tietoturvallisuussopimus tai vuoden 1994 sopimus, allekirjoittamista Suomen liityttyä Naton rauhankumppanuusohjelmaan (PfP) vuonna 1994. Suomen ja Naton välinen tietoturvallisuussopimus (*Security Agreement between Finland and the North Atlantic Treaty Organization)* allekirjoitettiin 22 päivänä syyskuuta 1994. Sopimuksessa sovittiin turvallisuusluokitellun aineiston vaihtamisesta ja suojaamisesta.

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.

Tietoturvallisuussopimuksella Suomi sitoutui luokittelemaan ja suojaamaan rauhankumppanuusohjelman puitteissa Natolta saadun aineiston sekä laatimaan turvallisuusselvityksen niistä henkilöistä, joilla on pääsy suojattuun aineistoon. Sopimuksen liitteenä oli selvitys Naton käyttämästä asiakirjojen turvallisuusluokittelusta sekä tiettyjen hallinnollisten kysymysten järjestämisestä sopimuksen toimeenpanemiseksi.

Samassa yhteydessä allekirjoitettiin Naton tilojen käyttöä koskeva käyttäytymissääntö (*Code of Conduct*), joka liittyi Suomen edustajien lisääntyvään liikkumiseen Naton tiloissa. Käyttäytymissäännön allekirjoittamalla kumppanuusmaa sitoutui olemaan käyttämättä Naton tiloja epäasialliseen toimintaan. Lisäksi ulkoasiainministeriön 13 päivänä syyskuuta 1994 tekemällä päätöksellä hyväksyttiin tietoturvallisuussopimukseen liittyvät kaksi hallinnollisluonteista asiakirjaa (turvallisuusluokiteltua tietoa koskevat minimistandardit ja toimeenpanojärjestely) ja nimettiin sopimuksessa edellytetyksi informaatio- ja asiakirjaturvallisuuskysymyksistä vastaavaksi hallintoviranomaiseksi (*Central Registry*) ulkoasiainministeriö.

Sopimus katsottiin voitavan tehdä tuolloin voimassa olleen valtiosäännön mukaisesti viranomaisten välisenä, niin sanottuna kansainvälisenä hallintosopimuksena, koska asiakirjaturvallisuutta koskeva sopimus luonnehdittiin käytännön yhteistyöhön liittyväksi hallinnollisluonteiseksi asiakirjaksi. Sopimuksen liitteineen ei katsottu olevan ristiriidassa Suomen lainsäädännön kanssa. Tämän johdosta päätös sopimuksen ja käyttäytymissäännön allekirjoittamisesta tehtiin lausuntokierroksen jälkeen ulkoasiainministeriössä. Sopimuksen allekirjoitti Suomen edustaja Natossa.

Vuonna 2004 Suomessa säädettiin laki kansainvälisistä tietoturvallisuusvelvoitteista (588/2004), jota sovelletaan erityissuojattaviin tietoaineistoihin. Näillä tarkoitetaan salassa pidettäviä asiakirjoja ja materiaaleja, jotka on toimitettu Suomen viranomaiselle ja joiden lähettäjä on kansainvälisen, Suomea sitovan sopimuksen tai muun kansainvälisen velvoitteen mukaisesti tehnyt niihin turvallisuusluokkaa koskevan merkinnän. Lakia voidaan soveltaa vain, jos kansainvälinen sopimus on saatettu Suomessa voimaan perustuslaissa säädetyllä tavalla tai jos kysymys on Suomea muutoin sitovasta kansainvälisestä velvoitteesta.

Koska Suomen ja Naton välistä tietoturvallisuussopimusta vuodelta 1994 ei ole saatettu Suomessa voimaan, sanottua lakia ei voi soveltaa Nato-turvallisuusluokitellun aineiston pitämiseen salassa. Sopimusta ei ole myöskään julkaistu Suomen säädöskokoelman sopimussarjassa. Sopimuksen nojalla Suomen

vastaanottamaa tietoa suojataan lähtökohtaisesti viranomaisten toiminnan julkisuudesta annetun lain (621/1999, jäljempänä julkisuuslaki) perusteella. Tällöin tiedon salassapito on riippuvainen siitä, aiheuttaisiko tiedon luovuttaminen kolmannelle osapuolelle vahinkoa suojattavalle edulle (ns. vahinkoedellytys). Vuoden 1994 tietoturvallisuussopimus ei myöskään vastaa enää täysin nykyisiä turvallisuusmääräyksiä, joten sopimusta oli tarpeen ajantasaistaa myös tältä osin.

Tilanteen korjaamiseksi Suomen Kansallinen turvallisuusviranomainen (NSA) keskusteli kesäkuussa 2011 Brysselissä alustavasti NOS:n kanssa tietoturvallisuussopimuksen uudistustarpeesta. Keskusteluissa ilmeni, että NOS ei ole valmis muuttamaan vuoden 1994 tietoturvallisuussopimusta, mutta sen täydentäminen ja tarkentaminen olisi mahdollista kirjeenvaihdolla tai muulla järjestelyllä. Tämän mukaisesti osapuolten välillä päädyttiin neuvottelemaan keväällä 2012 sopimusta täydentävä järjestely, joka allekirjoitettiin Helsingissä 3 päivänä heinäkuuta 2012. Kyseinen järjestely esitetään nyt saatettavaksi voimaan. Samanaikaisesti saatettaisiin voimaan myös vuonna 1994 tehty tietoturvallisuussopimus.

2 Nykytila ja sen arviointi

2.1 Laki kansainvälisistä tietoturvallisuusvelvoitteista

Laki kansainvälisistä tietoturvallisuusvelvoitteista (588/2004) säädettiin osana Suomen ja Saksan välisen tietoturvallisuussopimuksen sekä Euroopan avaruusjärjestön (ESA) tietoturvallisuussopimuksen voimaansaattamista (HE 66/2004 vp – EV 95/2004 vp). Laki katsottiin tarpeelliseksi muun ohella sen vuoksi, että kansainvälisten sopimusten panemiseksi täytäntöön on tarve poiketa asiakirjajulkisuuteen ja -turvallisuuteen perustuvista kansallisista järjestelyistä, jotka perustuvat pääosin julkisuuslakiin.

Käsitellessään edellä mainittua hallituksen esitystä, jossa esitettiin säädettäväksi muun muassa laki kansainvälisistä tietoturvallisuusvelvoitteista, hallintovaliokunta totesi, että puolustushallinnon alalla oli saadun selvityksen mukaan tehty useita hallinnollisiksi yhteisymmärrys-asiakirjoiksi otsikoituja sopimuksia eri valtioiden ja järjestöjen kanssa salassa pidettävien tietojen suojaamisesta. Sopimuksista suurin osa koski materiaalista yhteistyötä. Kansainvälinen yhteistyö oli lisääntynyt myös puolustushallinnossa, ja yhteistyötä tehtiin monella muullakin kuin ainoastaan materiaalisella alalla. Asiassa saadun selvityksen mukaan sopimukset olisi niitä uudistettaessa tarkoitus muuttaa valtiosopimuksiksi ja saattaa ne perustuslain edellyttämällä tavalla eduskunnan käsiteltäväksi. Hallintovaliokunta piti asiaa puolustusvaliokunnan tavoin tarpeellisena (HaVM 11/2004 vp). Valiokunnan kannanotto on osaltaan ollut pontimena hallituksen työlle tietoturvallisuusvelvoitteiden nostamiseksi lain tasolle mukaan lukien nyt kyseessä oleva vuoden 1994 tietoturvallisuussopimus.

Suomi on tehnyt tähän mennessä useita kahdenvälisiä tietoturvallisuussopimuksia, jotka on voimaansaatettu lailla. Ensimmäisen sopimuksen Suomi teki Länsi-Euroopan unionin (WEU) kanssa (SopS 41 ja 42/1998). Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain säätämisen yhteydessä vuonna 2004 hyväksyttiin tietoturvallisuussopimus Saksan liittotasavallan kanssa (SopS 96 ja 97/2004) sekä ESA:n kanssa (SopS 94 ja 95/2004). Vuotta myöhemmin allekirjoitettiin Suomen ja Ranskan välinen sopimus (SopS 66 ja 67/2005). Mainittujen sopimusten lisäksi Suomi on tehnyt tietoturvallisuussopimuksen Slovakian (SopS 116 ja 117/2007), Viron (SopS 12 ja 13/2008), Italian (SopS 23 ja 24/ 2008), Latvian (SopS 33 ja 34/2008), Puolan (SopS 46 ja 47/2008), Bulgarian (SopS 116 ja 117/2008), Slovenian (SopS 22 ja 23/2009), Tšekin (SopS 53 ja 54/2009) ja Espanjan (SopS 38 ja 39/2010) kanssa. Lisäksi Suomi on tehnyt tietoturvallisuussopimuksen Eurooppalaisen puolustusmateriaaliyhteistyöjärjestön (OCCAR) kanssa (SopS 109 ja 110/2008) sekä pohjoismaisen tietoturvallisuussopimuksen (SopS 128 ja 129/2010), jota sovelletaan tällä hetkellä väliaikaisesti Suomen, Ruotsin, Norjan ja Tanskan välillä (SopS 130/2010 ja 20/2012). Israelin kanssa Suomi on tehnyt sopimuksen puolustus- tai turvallisuushallintojen kesken

välitetystä turvallisuusluokitellusta tiedosta (SopS 34 ja 35/2012). Suomi on 10 päivänä toukokuuta 2012 hyväksynyt EU:n jäsenvaltioiden välillä toukokuussa 2011 allekirjoitetun sopimuksen turvallisuusluokitellun tiedon suojaamisesta, mutta sopimus ei ole toistaiseksi tullut voimaan. Eduskunta on hyväksynyt Luxemburgin kanssa tehdyn tietoturvallisuussopimuksen (HE 43/2012 vp EV 75/2012 vp). Kesäkuussa 2012 Suomi allekirjoitti tietoturvallisuussopimuksen sekä Ison-Britannian että Amerikan yhdysvaltojen kanssa. Suomi on lähiaikoina allekirjoittamassa tietoturvallisuussopimuksen myös Sveitsin kanssa. Kaikki edellä mainitut sopimukset on voimaansaatettu tai voimaansaatetaan perustuslain 8 luvun mukaisesti, minkä vuoksi kyseisten sopimusten nojalla vastaanotettuihin turvallisuusluokiteltuihin tietoihin sovelletaan lakia kansainvälisistä tietoturvallisuusvelvoitteista.

Lain yleinen soveltamisala

Lakia kansainvälisistä tietoturvallisuusvelvoitteista sovelletaan erityissuojattaviin tietoaineistoihin. Näillä tarkoitetaan salassa pidettäviä asiakirjoja ja materiaaleja, jotka on toimitettu Suomen viranomaiselle ja joiden lähettäjä on kansainvälisen, Suomea sitovan sopimuksen tai muun kansainvälisen velvoitteen mukaisesti tehnyt niihin turvallisuusluokkaa koskevan merkinnän. Määräysvalta luovutettuun tietoon säilyy luovutuksen jälkeenkin aineiston luovuttaneella osapuolella. Lakia voidaan soveltaa vain, jos kansainvälinen sopimus on saatettu Suomessa voimaan perustuslaissa säädetyllä tavalla tai jos kysymys on Suomea muutoin sitovasta kansainvälisestä velvoitteesta. Muuksi sitovaksi velvoitteeksi katsotaan lain perustelujen mukaan Euroopan unionin (EU) sitovat säädökset (esimerkiksi neuvoston päätös turvallisuussäännöistä EU:n turvallisuusluokiteltujen tietojen suojaamiseksi (2011/292/EU). Lakia ei siten tällä hetkellä sovelleta Naton Suomelle luovuttamaan turvallisuusluokiteltuun tietoaineistoon, koska vuoden 1994 tietoturvallisuussopimusta ei ole voimaansaatettu.

Lain soveltamisalan piiriin kuuluvia erityissuojattavia tietoaineistoja ovat myös 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.

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

Lain suhde julkisuuslainsäädäntöön

Kansainvälisistä tietoturvallisuusvelvoitteista annettuun lakiin sisältyy kansallisten asiakirjojen tietoturvallisuudesta annetuista säännöksistä poikkeavia säännöksiä. Keskeinen säännös on lain 6 §:n 1 momentti, jonka perusteella Suomen tietoturvallisuussopimuksen perusteella vastaanottama tieto on pidettävä salassa, ellei itse sopimuksesta muuta johdu. Säännös on poikkeus julkisuuslain sisältämästä vahinkoedellytyksestä. 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 elinkeinonhar-

joittaja on osapuolena turvallisuusluokitellussa sopimuksessa tai osallistuu tällaista sopimusta edeltävään hankintakilpailuun tai toimii tällaisen elinkeinonharjoittajan alihankkijana (1 §:n 2 mom.).

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

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

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

Lain täytäntöönpanoviranomaiset

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

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

Laissa kansainvälisistä tietoturvallisuusvelvoitteista on säännökset viranomaisia ja elinkeinonharjoittajaa koskevasta tiedonantovelvollisuudesta (16 §). Säännösten tarkoituksena on varmistaa, että toimivaltaiset turvallisuusviranomaiset saavat 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 sopimuksessa. Suomen tekemissä turvallisuusluokiteltujen tietojen vaihtoa koskevissa sopimuksissa on säännönmukaisesti määräys, joka rajoittaa luovutettujen tietojen käyttöä. Tämän mukaisesti erityissuojattavaa tietoaineistoa saa käyttää ja luovuttaa vain siihen tarkoitukseen, jota varten se on annettu, jollei se, joka on määritellyt aineiston turvallisuusluokan, ole antanut muuhun suostumustaan. 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 turvallisuusluokitusta vastaavista teknisistä turvallisuustoimenpiteistä valtioneuvoston asetuksella (9 §). Tietoturvallisuudesta valtionhallinnossa annetun valtioneuvoston asetuksen (681/2010), jäljempänä tietoturvallisuusasetus, 11 §:ssä on säädetty turvallisuusluokitusmerkintää koskevista erityissäännöksistä ja 12 §:ssä turvallisuusluokituksen vastaavuudesta.

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

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 henkilöstöturvallisuutta koskeva turvallisuusselvitys tehdään siten kuin turvallisuusselvityksistä annetussa laissa (177/2002) ja sen nojalla säädetään. Siten esimerkiksi selvityksen kohteena olevan henkilön oikeudet määräytyvät sanotun lain mukaisesti.

Kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa on kuitenkin kaksi säännöstä, jotka ovat erityissäännöksiä suhteessa turvallisuusselvityksistä annettuun lakiin. Suppea turvallisuusselvitys on mahdollista laatia muissakin kuin turvallisuusselvityksistä annetun lain 19 §:ssä luetelluissa tapauksissa, jos se on tarpeen kansainvälisen tietoturvallisuusvelvoitteen toteuttamiseksi (11 §:n 1 mom.). Toinen erityissäännös koskee viranomaisten toimivaltaa. Turvallisuusselvityksen tekee pääesikunta silloin kun turvallisuusselvityksen laatiminen on tarpeen puolustushallintoa tai puolustushankintoja koskevan kansainvälisen velvoitteen toteuttamiseksi. Muissa tapauksissa henkilöön liittyvien turvallisuusselvitysten laadinnasta huolehtii Suojelupoliisi (11 §:n 2 mom.).

Turvallisuusselvityksistä annetun lain 10 §:n 2 momentin mukaan turvallisuusselvitykseen ei saa sisällyttää selvityksen laatineen viranomaisen arviota selvityksen kohteena olevan henkilön luotettavuudesta tai sopivuudesta virkaan tai tehtävään, ellei lain 9 §:ssä tarkoitettu valtiosopimus tai muu kansainvälinen velvoite tätä edellytä. Koska pääsääntönä on, että turvallisuusselvitys ei sisällä arviota henkilön luotettavuudesta, laissa kansainvälisistä tietoturvallisuusvelvoitteista on erikseen säädetty henkilön luotettavuuden arvioinnista. Tällaisen arvion tekee turvallisuusselvityksen perusteella kansallinen turvallisuusviranomainen tai, jos turvallisuusviranomaisten välillä on niin sovittu, tehtävään määrätty turvallisuusviranomainen (11 §:n 3 mom.).

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

Yhteisöturvallisuusselvitys

Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 12 §:ssä säädetään yhteisöturvallisuusselvityksistä ja arvioista. Yhteisöturvallisuusselvityksellä varmistetaan elinkeinonharjoittajan toimitilojen ja käsittelykäytäntöjen asianmukaisuus sekä henkilöstön osaaminen. Elinkeinonharjoittajan luotettavuuden arvioinnilla varmistutaan erityisesti siitä, kuinka hyvin tämä pystyy huolehtimaan turvallisuusluokiteltujen tietojen suojaamisesta. Yhteisöturvallisuusmenettely ja siihen perustuva arvio toteutetaan pääosin elinkeinonharjoittajalta itseltään saatujen tietojen perusteella sekä tämän toimitilojen turvallisuuden kartoituksella, ja tarvittavista toimenpiteistä huolehditaan elinkeinonharjoittajan kanssa tehtävän sopimuksen avulla. Selvityksen laatii Suojelupoliisi. Pääesikunta huolehtii tehtävästä kuitenkin silloin, kun kysymys on puolustukseen liittyvästä hankinnasta. Selvitystä laadittaessa on otettava huomioon laissa yksilöidyt seikat, muun muassa se, miten turvallisuusluokiteltuja tietoja suojataan oikeudettomalta ilmitulolta, muuttamiselta ja hävittämiseltä, ja miten asiaton pääsy estetään tiloihin, joissa turvallisuusluokiteltuja tietoja käsitellään tai joissa harjoitetaan turvallisuusluokitellussa sopimuksessa tarkoitettua toimintaa. Viestintävirasto laatii tarvittaessa osana yhteisöturvallisuusselvitystä selvityksen ja arvion siitä, täyttävätkö elinkeinonharjoittajan tietojärjestelmät ja tietoliikenteen järjestelyt kansainvälisistä tietoturvallisuusvelvoitteista johtuvat vaatimukset.

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

2.2 Turvallisuusselvityksiä koskeva lainsäädäntö

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

Turvallisuusselvitys voidaan tehdä virkaan tai tehtävään hakeutuvasta, tehtävään tai koulutukseen otettavasta taikka virkaa tai tehtävää hoitavasta henkilöstä, ja se voi olla perusmuotoinen, laaja tai suppea. Turvallisuusselvitys tehdään laissa määritellyissä tapauk-

sissa, 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.

Turvallisuusselvityslain kokonaistarkistusta varten asetettu työryhmä on luovuttanut mietintönsä oikeusministerille 31 päivänä tammikuuta 2011. Työryhmälle annettuun tehtävään kuului turvallisuusselvityslain kehittäminen siten, että se vastaa Suomea sitovia velvoitteita ja kansainvälisesti yleisesti sovellettavia käytäntöjä. Uudistettua turvallisuusselvityslakia koskeva hallituksen esitys on tarkoitus antaa syysistuntokaudella 2012.

Edellä olevan perusteella Suomen lainsäädännön voidaan katsoa täyttävän hyvin turvallisuusluokitellun tiedon suojaamiseksi tarvittavat edellytykset.

3 Esityksen tavoitteet ja keskeiset ehdotukset

Esityksen tavoitteena on ensinnäkin saattaa lailla voimaan hallinnollinen järjestely koskien Suomen ja Pohjois-Atlantin liiton kesken vaihdettavan turvallisuusluokitellun tiedon suojaamista. Suomen ja Naton välillä heinäkuussa 2012 allekirjoitetun järjestelyn tarkoituksena on ajantasaistaa vuoden 1994 tietoturvallisuussopimus nykyisiä turvallisuusmääräyksiä vastaavaksi.

Toiseksi samalla lailla on tarkoitus saattaa voimaan myös vuoden 1994 sopimuksen määräykset, jotka uuden perustuslain ja sitä koskevan tulkintakäytännön johdosta nykyisin arvioidaan kuuluviksi lainsäädännön alaan. Tämä esitetään toteutettavaksi siten, että järjestelyä koskevaan voimaansaattamislakiin sisällytetään blankettisäännös, joka koskee vuoden 1994 sopimuksen voimaansaattamista. Myös laki kansainvälisistä tietoturvallisuusvelvoitteista edellyttää, että velvoite, johon sitä sovelletaan, on saatettu Suomessa voimaan perustuslaissa säädetyllä tavalla.

Vuoden 1994 tietoturvallisuussopimusta ei ole katsottu tarpeelliseksi uudelleen kansallisesti hyväksyä, koska sopimus on sen hyväksymishetkellä voimassa olleen valtiosäännön mukaisesti arvioitu kansainväliseksi hallintosopimukseksi ja sen mukaisesti hyväksytty ulkoasiainministeriön päätöksellä 13 päivänä syyskuuta 1994 allekirjoitusvaltuuksien myöntämisen yhteydessä. Vuoden 1994 tietoturvallisuussopimusta on sen allekirjoitushetkestä 22 päivästä syyskuuta 1994 lähtien tosiasiallisesti sovellettu Suomen ja Naton välillä. Vuoden 1994 tietoturvallisuussopimuksen osalta kyse on siten poikkeuksellisesta lainsäädännöllisestä ratkaisusta, jossa sopimuksen määräykset saatetaan jälkikäteen voimaan osana järjestelyä koskevaa voimaansaattamislakia.

Natolta saatua turvallisuusluokiteltua tietoa suojataan tällä hetkellä lähtökohtaisesti julkisuuslain säännösten perusteella, mikä merkitsee, että tiedon suojaaminen on riippuvainen siitä, aiheutuisiko tiedon luovuttamisesta kolmannelle osapuolelle vahinkoa (ns. vahinkoedellytys). Käytännössä Naton Suomelle luovuttamaa turvallisuusluokiteltua tietoa on suojattu tähän saakka julkisuuslain 24 § 1 momentissa säädettyjen salassapitoperusteiden (erityisesti Suomen kansainvälisiin suhteisiin liittyvät 1 ja 2 kohta, turvajärjestelyihin liittyvä 7 kohta sekä maanpuolustukseen liittyvä 10 kohta) perusteella ottaen huomioon vuoden 1994 sopimuksen määräykset. Tiedon suojaamisessa ei ole esiintynyt käytännön ongelmia.

Suomen turvallisuusluokiteltujen tietojen suojaamiseen Natossa vuoden 1994 sopi-

muksen jälkikäteisellä voimaansaattamisella ei ole vaikutusta, koska kyse on valtionsisäisestä toimenpiteestä.

Järjestely sisältää 16 artiklaa. Järjestelyn johdannossa viitataan Suomen ja Naton vuonna 1994 tekemän tietoturvallisuussopimuksen 4 artiklaan. Lisäksi järjestelyssä määrätään vastaavat turvallisuusviranomaiset (2 artikla), määritelmät (3 artikla), turvallisuusluokittelun tiedon merkitsemisestä (4 artikla), turvallisuusluokitellun tiedon suojaamisesta ja käytöstä (5 artikla), pääsystä turvallisuusluokiteltuun tietoon (6 artikla), turvallisuusluokitellun tiedon lähettämisestä (7 artikla), immateriaalioikeuksista (8 artikla), turvallisuusvaatimusten yksityiskohdista (9 artikla), järjestelyn noudattamisesta ja turvallisuustarkastuksista (19 artikla), vierailuista (11 artikla), tarkastusvierailuista (12 artikla), tiedon katoamisesta ja vaarantumisesta (13 artikla), kustannuksista (14 artikla), riitojen ratkaisusta (15 artikla) sekä loppumääräykset (16 artikla). Järjestely on tarkoitettu tulemaan voimaan Suomen ilmoittamana päivänä sen jälkeen, kun Suomi on saanut kansalliset hyväksymismenettelynsä päätökseen.

4 Esityksen vaikutukset

4.1 Vaikutukset kansalaisiin

Suomen ja Naton välisen järjestelyn ja vuoden 1994 tietoturvallisuussopimuksen voimaansaattamisen myötä Naton Suomeen toimittamiin turvallisuusluokiteltuihin tietoihin ja materiaaleihin sovellettaisiin lakia kansainvälisistä tietoturvallisuusvelvoitteista. Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain mukainen salassapito on riippuvainen sopimuksen määräyksistä, mikä merkitsee yleensä kattavampaa salassapitovelvoitetta kuin julkisuuslain säännökset. Suomen ja Naton välisessä järjestelyssä on kysymys asiakirjoista, joita toinen osapuoli pitää salassa pidettävinä ja jotka se on määritellyt ja merkinnyt korkean tietoturvallisuuden tasoa edellyttäviksi. Järjestelyn 5 artiklassa määrätään turvallisuusluokitellun tiedon salassapidosta. Artiklan 5.1.3 mukaan osapuolet eivät salli kolmansien osapuolten saada turvallisuusluokiteltua tietoa ilman tiedon lähettäjän kirjallista ennakkosuostumusta. Tämä merkitsee poikkeusta julkisuuslain yleistä etua koskevista salassapitosäännöksistä, joissa salassapito on useimmissa tapauksissa riippuvainen siitä, minkälaisia vaikutuksia tietojen antamisella olisi suojattavalle edulle. Tällaisia asiakirjoja on säännönmukaisesti pidettävä salaisina myös julkisuuslain 24 §:n 1 momentin 2 kohdan mukaan. 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 luokituksen oikeellisuudesta tai siitä, minkä asiakirjan tietojen vuoksi luokitusmerkintä on tehty, syntyy epäselvyyttä, viranomaisen on otettava yhteyttä asiakirjan laatineeseen osapuoleen. Edellä olevan perusteella voidaan arvioida, että Suomen ja Naton välisen järjestelyn ja tietoturvallisuussopimuksen voimaansaattamista koskeva lakiehdotus ei asiallisesti vaikuta kansalaisten tiedonsaantia vähentävästi suhteessa siihen, mitä tiedonsaanti yleisen lainsäädännön mukaan on.

Ehdotetun voimaansaattamislain hyväksyminen ei tarkoittaisi sitä, että kansalaisten yksityiselämän ja henkilötietojen suojaa kavennettaisiin aikaisempaan verrattuna, koska henkilöllisyysturvallisuusselvityksiin sovelletaan aina turvallisuusselvityksistä annettua lakia. Voimaansaattamissäädösten yhteydessä järjestely ja vuoden 1994 tietoturvallisuussopimus julkaistaisiin myös Suomen säädöskokoelman sopimussarjassa, mikä merkitsee myös sitä, että sopimustekstit ovat tämän jälkeen yleisesti sähköisesti saatavilla.

4.2 Vaikutukset elinkeinoelämään

Järjestely ja sopimus antavat Suomen elinkeinoelämälle mahdollisuuden saada sellaisia tilauksia tai osallistua sellaisiin hankkeisiin, joiden toteuttaminen edellyttää pääsyä Naton turvallisuusluokiteltuihin tietoihin.

4.3 Taloudelliset vaikutukset

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

4.4 Vaikutukset hallintoon ja viranomaisten toimintaan

Esitykseen sisältyvän järjestelyn ja lain hyväksymisestä ei aiheudu hallintoa koskevia muutosvelvoitteita tai -tarpeita. Naton tietoturvallisuusmääräyksiä on sovellettu Suomessa jo vuoden 1994 tietoturvallisuusopimuksen perusteella. Järjestely lisää jonkin verran kansallisen turvallisuusviranomaisen ja määrättyjen turvallisuusviranomaisten niitä tehtäviä, jotka kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 4 §:n mukaisesti kuuluvat näille viranomaisille.

5 Asian valmistelu

Suomen kansallinen turvallisuusviranomainen (NSA) keskusteli kesäkuussa 2011 Brysselissä alustavasti NOS:n kanssa tietoturvallisuussopimuksen uudistustarpeesta. Suomen lähtökohtana neuvotteluissa oli, että vuoden 1994 sopimusta voitaisiin muuttaa ja muutettu sopimus saatettaisiin Suomessa valtiosopimuksena voimaan. Keskusteluissa ilmeni, että NOS ei ole valmis muuttamaan vuoden 1994 sopimusta, mutta sen täydentäminen ja tarkentaminen olisi mahdollista kirjeenvaihdolla tai muulla järjestelyllä.

Valtioneuvoston yleisistunto asetti valtuuskunnan neuvotteluja varten 8 päivänä maaliskuuta 2012. Valtuuskunnan puheenjohtajana toimi ulkoasiainministeriön edustaja (NSA). Valtuuskunnan jäseninä ja asiantuntijoina oli edustajia ulkoasiainministeriöstä, oikeusministeriöstä, puolustusministeriöstä, Suojelupoliisista ja Viestintävirastosta sekä Suomen erityisedustustosta Pohjois-Atlantin liitossa (NAE).

Valtuuskunta neuvotteli vuoden 1994 tietoturvallisuussopimusta täydentävän järjestelyn Brysselissä huhtikuussa 2012 sopimuksen 4 artiklan perusteella. Järjestelyllä ajantasaistetaan vuoden 1994 sopimus siten, että siinä otetaan huomioon tarvittavilta osin kansainvälisen tietoturvallisuuslain säännökset sekä voimassa olevat turvallisuusmääräykset. Tarkoituksena on, että järjestely yhdessä vuoden 1994 sopimuksen kanssa saatettaisiin voimaan perustuslain 8 luvun mukaisesti. Järjestelyn ja sopimuksen voimaansaattaminen edellyttää eduskunnan hyväksyntää, koska velvoitteet sisältävät lainsäädännön alaan kuuluvia määräyksiä.

Hallituksen esitys on valmisteltu ulkoasiainministeriössä. Sopimuksen valmisteluun ja neuvotteluihin on osallistunut edustajia ulkoasiainministeriöstä, oikeusministeriöstä, puolustusministeriöstä, Viestintävirastosta ja Suojelupoliisista. Esityksestä on pyydetty lausunnot oikeusministeriöltä, puolustusministeriöltä, sisäasiainministeriöltä, valtiovarainministeriöltä, liikenne- ja viestintäministeriöltä, työ- ja elinkeinoministeriöltä, Suojelupoliisilta ja Viestintävirastolta. Lausunnoissa on puollettu esitettyä järjestelyä.

YKSITYISKOHTAISET PERUSTELUT

1 Suomen ja Pohjois-Atlantin liiton kesken vaihdettavan turvallisuusluokitellun tiedon suojaamisesta tehty hallinnollinen järjestely ja sen suhde Suomen lainsäädäntöön

1 artikla. *Johdanto.* Järjestelyn johdannossa viitataan vuonna 1994 Suomen ja Naton välillä tehtyyn tietoturvallisuussopimukseen ja sen 4 artiklaan, jossa määrätään hallinnollisista järjestelyistä, jotka koskevat muun muassa vaihdettavien tietojen vastavuoroisen suojaamisen vaatimuksia sekä Naton turvallisuustoimiston ja Suomen turvallisuusviranomaisen yhteyksiä.

Neuvoteltaessa uutta järjestelyä NOS:n kanssa käytiin keskustelua siitä, olisiko järjestelyssä mahdollista todeta vuoden 1994 sopimusta selkeämmin, että järjestelyn soveltamisalan on tarkoitus kattaa kaikki se yhteistyö, mitä Suomi tekee Naton kanssa, erityisesti kriisinhallintaoperaatioihin liittyvä yhteistyö. Tämän vuoksi Suomi esitti, että järjestelyn johdantoon olisi lisätty maininta "ja ottaen huomioon poliittinen ja turvallisuuteen liittyvä yhteistyö osapuolten välillä". NOS ei ollut halukas muutokseen ja painotti, että PfP-yhteistyön voidaan katsoa kattavan kaikki ne yhteistyömuodot, joita Suomella on Naton kanssa.

2 artikla. *Turvallisuusviranomaiset.* Järjestelyn 2 artiklassa määrätään täytäntöönpanojärjestelystä vastaavista osapuolten turvallisuusviranomaisista, joita ovat Naton taholta Naton turvallisuustoimisto (NOS) ja Suomen taholta Kansallinen turvallisuusviranomainen (NSA). Osapuolet sitoutuvat toimittamaan toisilleen tarkemmat turvallisuusviranomaisten yhteystiedot. Sopimusmääräys vastaa kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 4 §:n 1 momenttia. Määräys on siten toteava, eikä sen siten ole katsottava edellyttävän eduskunnan hyväksymistä. Kansallisen turvallisuusviranomaisen lisäksi Suomessa toimii määrättyjä turvallisuusviranomaisia (Designated Security Authority, DSA), joita ovat kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 4 §:n mukaisesti puolustusministeriö, pääesikunta, Suojelupoliisi ja Viestintävirasto.

3 artikla. *Määritelmät.* Artiklassa määritellään järjestelyn keskeiset termit seuraavasti: Turvallisuusluokitellulla tiedolla tarkoitetaan kaikkea jommaltakummalta osapuolelta peräisin olevaa tai jommankumman osallistujan tuottamaa tai vaihtamaa tietoa ja aineistoa, johon sovelletaan turvallisuusluokitusta. Tällaiseen tietoon luetaan kuuluvaksi myös asiakirjat, laitteet, aineet ja muut esineet kaikissa muodoissaan sekä kaikki tällaisen tiedon tai aineiston jäljennökset ja käännökset riippumatta siitä, missä muodossa ja millä tavalla tieto välitetään. Käsitteen määritelmä on sopusoinnussa kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 2 §:n 1 kohdan kanssa. Luovuttavalla osapuolella tarkoitetaan tiedon omistavaa osapuolta. Välittävällä osapuolella tarkoitetaan tiedon välittävää osapuolta. Vastaanottavalla osapuolella tarkoitetaan osapuolta, joka saa tiedon välittävältä osapuolelta. Kolmas osapuoli tarkoittaa muuta henkilöä tai yhteisöä kuin osapuolta.

4 artikla. *Turvallisuusluokitellun tiedon merkitseminen*. Artiklassa määrätään tiedon luovuttavan osapuolen velvollisuudesta merkitä luovuttamaansa tietoon artiklan 3 kohdassa määrätty turvallisuusluokka. Jos merkinnän tekeminen osoittautuu käytännössä mahdottomaksi, luovuttava osapuoli ilmoittaa luokan erikseen tiedon vastaanottavalle osapuolelle. Luovutetun tiedon omistajuus, leima taikka sen turvallisuusluokka ei muutu luovutuksessa.

Artiklan 3 kohdassa määritellään, miten Suomen ja Naton turvallisuusluokituksen tasot vastaavat toisiaan. Suomen turvallisuusluokkaa "SALAINEN" ("HEMLIG") vastaa Naton turvallisuusluokka "NATO SECRET". Tähän luokkaan kuuluvat Suomessa tiedot, joiden luvaton ilmitulo voi aiheuttaa merkittävää vahinkoa maanpuolustukselle, turvalli-

suudelle, kansainvälisille suhteille tai muille yleisille eduille. Suomen turvallisuusluokkaa "LUOTTAMUKSELLINEN" (”KONFIDENTIELL”) vastaa Naton ”NATO CONFIDENTIAL”, jolla tarkoitetaan Suomessa tietoja, joiden luvaton ilmitulo voi aiheuttaa vahinkoa maanpuolustukselle, turvallisuudelle, kansainvälisille suhteille tai muille yleisille eduille. Suomen turvallisuusluokkaa "KÄYTTÖ RAJOITETTU" (”BEGRÄNSAD TILLGÅNG”) vastaa Naton ”NATO RESTRICTED”, joiden luvaton ilmitulo voi aiheuttaa haittaa yleisille eduille tai heikentää viranomaisen toimintaedellytyksiä. Suomenkielisiä turvallisuusluokitusmerkintöjä vastaavat ruotsinkieliset merkinnät on lueteltu edellä suluissa.

Artiklan 4 kohdan mukaan osapuolten tuottamaan turvallisuusluokiteltuun tietoon, joka sisältää myös toisen osapuolen antamaa turvallisuusluokiteltua tietoa, merkitään etuliitteeksi SUOMI/NATO tai NATO/SUOMI ja sen jälkeen asianmukainen turvallisuusluokka, jotta asiakirjan voidaan todeta sisältävän yhteisesti omistettua turvallisuusluokiteltua tietoa.

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.

5 artikla. *Turvallisuusluokitellun tiedon suojaaminen ja käyttö.* Artiklan 1 kohdassa määrätään niistä menettelytavoista, joita osapuolet soveltavat vastaanottamansa turvallisuusluokitellun tiedon suojaamiseen ja käyttöön. Ensimmäisen alakohdan mukaan turvallisuusluokitellun tiedon vastaanottava osapuoli antaa tiedolle vähintään samantasoisen fyysisen ja oikeudellisen suojan kuin omalle vastaavaan turvallisuusluokkaan kuuluvalle tiedolleen. Tiedon vastaanottava osapuoli sitoutuu 2 alakohdan mukaan siihen, ettei tietoa käytetä muuhun kuin siihen tarkoitukseen, jota varten se luovutetaan, ellei tiedon lähettävä osapuoli anna ennakolta muuhun suostumustaan. Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 6 §:n 2 momentissa säädetään vastaavasti, että turvallisuusluokiteltua tietoa saa käyttää ainoastaan siihen tarkoitukseen, jota varten se on annettu. Tiedon paljastamiseen tai luovuttamiseen kolmannelle osapuolelle on saatava 3 alakohdan mukaan luovuttavan osapuolen kirjallinen ennakkosuostumus. Neljännessä alakohdassa edellytetään, että

vastaanottava osapuoli noudattaa niitä lisärajoituksia, joita luovuttava osapuoli tai joku muu tämän puolesta voi asettaa turvallisuusluokitellun tiedon käyttämiselle, paljastamiselle ja luovuttamiselle sekä pääsylle tähän tietoon. Vastaanottavalla osapuolella ei ole 5 alakohdan mukaan oikeutta alentaa luovuttavan osapuolen merkitsemää turvallisuusluokkaa ilman tämän antamaa kirjallista ennakkosuostumusta. Luovuttava osapuoli on velvollinen 6 alakohdan mukaan ilmoittamaan, jos luovutetun tiedon turvallisuusluokka myöhemmin muuttuu (esimerkiksi luokka alenee tai tieto luokitellaan uudelleen). Vastaanottava osapuoli on 7 alakohdan mukaan velvollinen toteuttamaan kaikki tarvittavat toimet suojatakseen turvallisuusluokiteltua tietoa luvattomalta paljastamiselta. Turvallisuusluokitusmerkinnöistä on säädetty kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 8 §:ssä sekä tietoturvallisuusasetuksen 11 ja 12 §:ssä.

Artiklan 2 kohdassa edellytetään, että kumpikin osapuoli on tietoinen toistensa turvallisuusluokitellun tiedon käsittelyä koskevista vähimmäisvaatimuksista. Naton osalta nämä vaatimukset esitetään asiakirjassa C-M(2002)49, "*Security within the North Atlantic Treaty Organisation*", jäljempänä Naton turvallisuussäännöt, ja sitä tukevissa ohjeissa (*directives*) sekä erityisesti tulkintaohjeessa (supporting document) AC/35-D/1038, "*Supporting Document on the Security Protection of NATO Information Released to Non-NATO Nations and International Organisations*". Tulkintaohje on tarkoitettu Natoon kuulumattomien maiden sellaisten turvallisuusviranomaisten käyttöön, joiden tehtävänä on varmistaa Naton luovuttaman turvallisuusluokitellun tiedon suojaaminen ja sitä tulkitaan yhdessä Naton turvallisuussääntöjen kanssa. Tulkintaohje sisältää turvallisuusmääräykset koskien organisaatioturvallisuutta, henkilöstöturvallisuutta, fyysistä turvallisuutta, tietoturvallisuutta, tietojärjestelmäturvallisuutta, yritysturvallisuutta ja tietoturvallisuusloukkauksia. Suomen osalta turvallisuusluokitellun tiedon käsittelyä koskevat vähimmäisvaatimukset esitetään asiaa koskevissa Suomen säädöksissä ja määräyksissä. Tämä tarkoittaa erityisesti lakia kansainvälisistä tietoturvallisuusvelvoitteista ja tietoturvallisuusasetusta.

Kun tietoa ei enää tarvita siihen tarkoitukseen, jota varten se on annettu, vastaanottava osapuoli on 3 kohdan mukaan velvollinen joko palauttamaan tiedon luovuttavalle osapuolelle siten kuin nämä osapuolet keskenään sopivat tai hävittämään tiedon vastaanottavan osapuolen menettelyjä noudattaen. Velvollisuudesta pitää huolta erityissuojattavan tietoaineiston suojaamisesta sen turvallisuusluokkaa vastaavalla tavalla muun muassa sitä hävitettäessä on säädetty kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 9 §:n 1 momentissa. Pykälän 2 momentissa on annettu valtuus säätää valtioneuvoston asetuksella (tietoturvallisuusasetus) eri turvallisuusluokkia vastaavista turvallisuustoimenpiteistä. Käsittelyä koskevat määräykset on siten Suomessa säädetty asetuksentasoisina.

Artiklan 4 kohta mahdollistaa turvallisuusluokitellun tiedon suojaamista koskevista lisävaatimuksista sopimisen osapuolten välillä. Lisävaatimukset koskisivat lähinnä teknisiä käytännön järjestelyjä. Artiklan 5 kohdan mukaan tiedon luovuttava osapuoli pidättää itsellään oikeuden kieltäytyä välittämästä turvallisuusluokiteltua tietoaan.

6 artikla. *Pääsy turvallisuusluokiteltuun tietoon*. Järjestelyn perusteella sallitaan pääsy turvallisuusluokiteltuun tietoon vain sellaisille Suomen kansalaisille ja Naton virkamiehille, joilla on asianmukaisen tason turvallisuusselvitys (1 kohdan 2 alakohta), jotka tarvitsevat tietoa työtehtäviensä suorittamiseen (tiedonsaantitarpeen periaate) (1 kohdan 3 alakohta), ja joille on selostettu noudatettavat turvallisuusmenettelyt ja jotka ovat tunnustaneet turvallisuusvelvoitteensa. Määräykset ovat sopusoinnussa kansainvälisen tietoturvallisuusvelvoitteista annetun lain 6 §:n 3 momentin kanssa, jossa sallitaan tietoaineistoon pääsy vain niille henkilöille, jotka tarvitsevat tietoja tehtävänsä hoitamiseen. Kansainvälisen tietoturvallisuusvelvoitteen edellyttämä henkilöiden luotettavuuden varmistaminen toteutetaan Suomessa turvallisuusselvityksistä annetun lain sekä kansainvälisistä tietoturvallisuusvelvoitteista annetun

lain 11 §:n mukaisesti. Henkilöturvallisuusselvityksen laatii pääesikunta silloin, kun sen laatiminen on tarpeen puolustushallintoa tai puolustushankintoja koskevan velvoitteen toteuttamiseksi. Muutoin selvityksen laatii Suojelupoliisi.

7 artikla. *Turvallisuusluokitellun tiedon välittäminen.* Osapuolet välittävät 1 kohdan mukaan turvallisuusluokitellun tiedon toisilleen välittävän osapuolen turvallisuusmääräysten ja -menettelyjen mukaisesti. Turvallisuusluokiteltu tieto välitetään 2 kohdan mukaan Suomen tai Naton virallisia kanavia käyttäen, elleivät osapuolet muuta sovi. Osapuolet voivat 3 kohdan perusteella välittää turvallisuusluokiteltua tietoa myös sähköisesti, mitä varten Naton turvallisuustoimisto ja Suomen kansallinen tietoturvallisuusviranomainen luovat keskenään erityiset menettelyt. Määräys on sopusoinnussa tietoturvallisuusasetuksen 18 ja 19 §:n kanssa.

Kansallisena tietoturvallisuusviranomaisena Suomessa toimii kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 4 §:n 3 momentin mukaan tietojärjestelmien ja tietoliikenteen tietoturvallisuutta koskevissa asioissa Viestintävirasto. Sopimuksen 7 artiklan 3 kohdan nojalla Viestintäviraston tehtävänä on luoda yhdessä Naton turvallisuustoimiston kanssa erityiset menettelyt turvallisuusluokitellun tiedon sähköiseen välittämiseen järjestelyn osapuolten välillä. Viestintävirasto voi määritellä Naton turvallisuustoimiston kanssa, millaisia tieto- ja viestintäjärjestelmiä koskevia teknisiä menettelyjä turvallisuusluokitellun tiedon sähköisessä välittämisessä voidaan toteuttaa. Artiklan 3 kohdan nojalla Viestintäviraston tehtäväksi ei sen sijaan tulisi rakentaa, ylläpitää tai hallinnoida Suomen ja Naton välisessä tiedonvaihdossa käytettäviä sähköisiä tietoverkkoja tai tietojärjestelmiä.

8 artikla. *Immateriaalioikeudet.* Artiklan mukaan järjestely ei vaikuta kummankaan osapuolen olemassaoleviin tai tuleviin immateriaalioikeuksiin (mukaan lukien patentit ja tekijänoikeudet), jotka liittyvät turvallisuusluokiteltuun tietoon.

9 artikla. *Turvallisuusvaatimusten yksityiskohdat*. Määräys koskee tietojenvaihtoa, jolla varmistetaan, että osapuolilla on tieto toistensa turvallisuusvaatimuksia koskevista säännöistä ja menettelyistä. Osapuolet antavat toisilleen tiedot turvallisuusluokitellun tiedon suojaamista koskevista turvallisuusvaatimuksistaan, -käytännöistään ja -menettelyistään. Osapuolet ilmoittavat toisilleen kirjallisesti turvallisuusvaatimustensa, -käytäntöjensä ja -menettelyjensä muutoksista, jotka vaikuttavat siihen, miten turvallisuusluokiteltua tietoa suojataan.

10 artikla. *Järjestelyn noudattaminen ja turvallisuustarkastukset*. Artiklan 1 kohdassa edellytetään, että kumpikin osapuoli varmistaa laitostensa, organisaatioidensa ja henkilöstönsä noudattavan järjestelyä. Osapuolet suorittavat tarvittavat turvallisuustarkastukset varmistaakseen, että asianmukaisia turvallisuusmääräyksiä ja –menettelyjä noudatetaan.

11 artikla. *Vierailut - Yleistä.* Artiklaa sovelletaan vierailuihin, joihin liittyy mahdollisuus saada turvallisuusluokiteltua tietoa. Vierailut, jotka edellyttävät pääsyä turvallisuusluokiteltuun tietoon tai turvallisuusselvitystä edellyttävään laitokseen, sallitaan artiklan 1 kohdan mukaan ainoastaan sellaisille henkilöille, joilla on voimassa oleva todistus asianmukaisen tason turvallisuusselvityksestä ja jotka tarvitsevat pääsyä kyseiseen tietoon tai laitokseen suorittaakseen työtehtäviään. Turvallisuusviranomaisen nimeämän vierailevan osapuolen toimivaltainen turvallisuuselin toimittaa 2 kohdan mukaan vierailupyynnöt hyväksyttäväksi asianomaisen turvallisuusviranomaisen hyväksymälle isäntänä toimivan osapuolen toimivaltaiselle turvallisuuselimelle. Pyynnöt on toimitettava vähintään kaksikymmentä (20) työpäivää ennen ehdotetun vierailun ajankohtaa.

Pyynnöistä on käytävä ilmi 3 kohdassa määrätyt tiedot: ehdotetun vierailun tarkoitus; vierailun ehdotettu ajankohta ja kesto; yksityiskohtaiset tiedot vierailun kohteena olevista laitoksista, organisaatioista ja henkilöstöstä; vierailusta lisätietoja antavan henkilön yhteystiedot, vierailun kohteena olevien laitosten, toimitilojen ja organisaatioiden yhteystiedot sekä vierailuun liittyvän turvallisuusluokitellun tiedon arvioitu taso. Vierailijoista on annettava seuraavat tiedot: vierailijan koko nimi, syntymäaika ja –paikka, kansalaisuus ja passin numero, vierailijan edus-

tama taho sekä vierailijan tehtävä (tarvittaessa arvoasema) sekä kunkin vierailijan todistus henkilöturvallisuusselvityksestä, sen antamispäivä, voimassaoloaika ja mahdolliset rajoitukset.

Artiklan 4 kohdassa edellytetään, että vierailupyyntöjen tueksi toimitetaan todistukset kunkin vierailijan turvallisuusselvityksen tasosta. Kaikkien vierailijoiden on 5 kohdassa määrätyn mukaisesti noudatettava asianmukaisia turvallisuusmääräyksiä ja isäntänä toimivan osapuolen sovellettavia laitoskohtaisia ohjeita.

Artiklan 6 kohdassa todetaan, ettei mikään vierailuja koskevan artiklan määräys rajoita kummankaan osapuolen oikeutta sallia toisen osapuolen vierailijoiden pääsyä turvallisuusluokiteltuun tietoon tai kulkua valvotuille alueille tai muihin laitoksiin milloin tahansa hyväksytyn vierailun aikana, jos isäntänä toimiva osapuoli haluaa sallia tällaisen pääsyn tai kulun.

12 artikla. *Tarkastusvierailut.* Artiklassa mahdollistetaan osapuolten väliset vierailut sen varmistamiseksi, että turvallisuusluokiteltua tietoa säilytetään ja käsitellään keskinäisesti päätettyjen vähimmäisvaatimusten mukaisesti. NOS ja Suomen NSA päättävät keskenään vastavuoroisista vierailuista ja suorittavat niitä ottaen huomioon 11 artiklassa määrätyt edellytykset vierailuille. Vierailujen toteuttamiseen liittyvät säännökset ovat kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 18 §:ssä.

13 artikla. *Katoaminen ja vaarantuminen.* Artiklassa osapuolet sitoutuvat ilmoittamaan välittömästi turvallisuusluokitellun tiedon luovuttaneelle tai välittäneelle osapuolelle, jos tällaista tietoa katoaa tai se vaarantuu tai sen epäillään kadonneen tai vaarantuneen. Vastaanottava osapuoli tutkii välittömästi tällaisen katoamisen tai vaarantumisen ja ilmoittaa luovuttavalle osapuolelle ja/tai välittävälle osapuolelle viipymättä tutkinnan tuloksista ja toteutetuista tai toteutettavista korjaustoimista. Kansallisesti artiklan velvoitteiden toteuttamiseksi tarvittavat säännökset sisältyvät kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 19 §:ään.

14 artikla. *Kustannukset***.** Artiklan mukaan kumpikin osapuoli vastaa omista kustannuksistaan, jotka niille aiheutuvat järjestelystä johtuvien velvoitteiden täyttämisestä.

15 artikla. *Riitojen ratkaiseminen*. Artiklan mukaan kaikki järjestelyn tulkintaan tai soveltamiseen liittyvät osapuolten väliset riidat ratkaistaisiin yksinomaan osapuolten välisin kuulemisin ja neuvotteluissa. Riitoja ei ole mahdollista saattaa kansallisten tai kansainvälisten tuomioistuinten tai kolmansien osapuolten ratkaistaviksi.

16 artikla. *Järjestelyn voimaantulo, uudelleentarkastelu, muuttaminen, kesto ja päättyminen*. Artiklan 1 kohta koskee järjestelyn voimaantuloa. Sen mukaisesti järjestely tulee voimaan sinä päivänä, jonka Suomi ilmoittaa Natolle sen jälkeen, kun Suomi on saattanut kansalliset hyväksymistoimensa loppuun. Koska järjestely edellyttää voimaantullakseen Suomessa eduskunnan suostumusta ja tasavallan presidentin hyväksyntää perustuslain 8 luvun säännösten mukaisesti, tarkoituksena on, että Natolle ilmoitetaan järjestelyn voimaantulopäiväksi tietty päivä vasta kyseisten päätösten jälkeen. Päivämäärä on tarkoitus ajoittaa siten, että jäisi riittävästi aikaa järjestelyn ja lain voimaansaattamiseksi valtioneuvoston asetuksella.

Artiklan 2 kappale sisältää määräyksen järjestelyn toimivuuden tarkastelusta ja muuttamisesta. Muuttaminen edellyttää molempien osapuolten kirjallista suostumusta. Jos järjestely päättyy, sen nojalla luovutettua tietoa suojataan edelleenkin 3 kohdan perusteella niiden voimassa olevien vastuiden ja velvoitteiden mukaisesti, jotka liittyvät välitetyn turvallisuusluokitellun tiedon suojaamiseen ja käyttöön.

2 Tietoturvallisuussopimus Suomen ja Pohjois-Atlantin liiton välillä ja sen suhde Suomen lainsäädäntöön

Johdanto. Sopimuksen johdannossa kiinnitetään huomiota siihen, että Suomi toimii Pohjois-Atlantin yhteistyöneuvoston/Naton rauhankumppanuuden kumppanivaltiona. Lisäksi johdannossa todetaan, että osapuolet ovat sopineet neuvottelevansa keskenään po-

liittisista ja turvallisuuteen liittyvistä asioista sekä laajentavansa ja vahvistavansa poliittista ja sotilaallista yhteistyötä kaikkialla Euroopassa. Tehokas yhteistyö sanotuissa asioissa edellyttää arkaluonteisten ja/tai salassa pidettävien tietojen vaihtamista osapuolten kesken. Naton käsitys PfP –yhteistyöstä on varsin laaja ja se kattaa ne yhteistyömuodot, joita Suomella on Naton kanssa. Asiaa on selostettu tarkemmin edellä järjestelyn johdannon perusteluissa.

1 artikla. Artikla sisältää uutta järjestelyä periaatteiltaan vastaavan määräyksen turvallisuusluokitellun tiedon suojaamisesta. Määräys on kirjoitettu kuitenkin uutta järjestelyä yleisemmällä tasolla. Artiklan i kohdassa osapuolet sitoutuvat suojaamaan ja turvaamaan toisen osapuolen tiedon ja aineiston. Artiklan ii kohdassa osapuolet pyrkivät kaikin keinoin varmistamaan, että jos tällaiset tiedot ja aineistot on turvallisuusluokiteltu, niillä säilytetään ne turvallisuusluokat, jotka jompikumpi osapuoli on määrännyt siltä peräisin oleville tiedoille ja aineistoille. Lisäksi turvallisuusluokiteltu tieto ja aineisto on suojattava yhteisesti sovittuja vaatimuksia noudattaen. Yhteisiin vaatimuksiin viitataan myös uuden järjestelyn 5 artiklan 2 kohdassa. Tällä hetkellä järjestelyt tarkoittavat Naton asiakirjaa C-M(2002)49, “Security within the North Atlantic Treaty Organisation”, ja sitä tukevia ohjeita, erityisesti ohje AC/35-D/1038, “Supporting Document on the Security Protection of NATO Information Released to Non-NATO Nations and International Organisations”. Suomen osalta vaatimukset tarkoittavat erityisesti lakia kansainvälisistä tietoturvallisuusvelvoitteista ja tietoturvallisuusasetusta. Asiakirjojen sisältöä on selostettu tarkemmin edellä järjestelyn 5 artiklan 2 kohdan yksityiskohtaisissa perusteluissa.

Artiklan iii kohdassa osapuolet sitoutuvat siihen, etteivät ne käytä vaihdettuja tietoja ja aineistoja muihin kuin niihin tarkoituksiin, joista on määrätty asianomaisissa ohjelmissa ja näitä ohjelmia koskevissa päätöksissä ja päätöslauselmissa. Osapuolet sitoutuvat iv kohdan mukaan myös siihen, etteivät ne paljasta tällaisia tietoja ja aineistoja kolmansille osapuolille ilman luovuttajan suostumusta.

Velvollisuudesta pitää huolta erityissuojattavan tietoaineiston suojaamisesta sen turvallisuusluokkaa vastaavalla tavalla muun muassa sitä hävitettäessä on säädetty kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 9 §:n 1 momentissa. Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 8 §:n mukaan erityissuojattavaan tietoaineistoon on tehtävä 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.

2 artikla. Artiklassa on määrätty henkilöstöturvallisuusselvityksistä. Suomen hallitus hyväksyy sitoumuksen tehdä kaikista kansalaisistaan, jotka työtehtäviään suorittaessaan tarvitsevat pääsyä Pohjois-Atlantin yhteistyöneuvoston tai rauhankumppanuuden ohjelmien mukaisesti vaihdettaviin tietoihin tai aineistoihin tai saattavat päästä niihin, asianmukainen turvallisuusselvitys ennen kuin heille annetaan pääsy tällaisiin tietoihin ja aineistoihin. Turvallisuusselvitysmenettelyt on suunniteltava sellaisiksi, että niissä määritetään, voidaanko henkilölle hänen lainkuuliaisuutensa ja luotettavuutensa huomioon ottaen sallia pääsy turvallisuusluokiteltuihin tietoihin vaarantamatta niiden turvallisuutta.

Kansainvälisen tietoturvallisuusvelvoitteista annetun lain 6 §:n 3 momentissa sallitaan pääsy turvallisuusluokiteltuun tietoaineistoon vain niille henkilöille, jotka tarvitsevat tietoja tehtävänsä hoitamiseen. Kansainvälisen tietoturvallisuusvelvoitteen edellyttämä henkilöiden luotettavuuden varmistaminen toteutetaan Suomessa turvallisuusselvityksistä annetun lain sekä kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 11 §:n mukaisesti. Henkilöturvallisuusselvityksen laatii pääesikunta silloin, kun sen laatiminen on tarpeen puolustushallintoa tai puolustushankintoja koskevan velvoitteen toteuttamiseksi. Muutoin selvityksen laatii Suojelupoliisi.

3 artikla. Artiklassa määrätään, että NOS (Naton turvallisuustoimisto) vastaa yhteis-

työneuvosto- tai rauhankumppanuusyhteistyössä vaihdettavia turvallisuusluokiteltuja tietoja koskevista turvallisuusjärjestelyistä Naton puolelta.

4 artikla. Artiklassa määrätään Suomen puolen turvallisuusviranomaisesta. Suomen puolelta viranomaiseksi on ilmoitettu vuonna 1994 ulkoasiainministeriö (nykyään NSA). Lisäksi artiklassa edellytetään, että Suomen ja Naton välillä tehdään erilliset hallinnolliset järjestelyt, jotka koskevat muun muassa vaihdettavien tietojen vastavuoroisen suojaamisen vaatimuksia sekä Suomen turvallisuusviranomaisen ja Naton turvallisuustoimiston välisiä yhteyksiä. Kyseisiä järjestelyjä ja yhteyksiä koskevia asiakirjoja on selostettu jäljempänä.

5 artikla. Artiklassa edellytetään, että ennen kuin Suomen ja Naton välillä vaihdetaan turvallisuusluokiteltuja tietoja, 3 ja 4 artiklassa mainittujen turvallisuusviranomaisten on vastavuoroisesti todettava hyväksymällään tavalla, että tiedot vastaanottava osapuoli suojaa tietoa samalla tavalla kuin vastaavaan turvallisuusluokkaan kuuluvaa omaa tietoaan.

3 Lakiehdotuksen perustelut

1 §. Pykälässä säädettäisiin, että vuonna 1994 Suomen ja Naton välillä tehdyn tietoturvallisuussopimuksen ja Suomen ja Naton vuonna 2012 tehdyn hallinnollisen järjestelyn lainsäädännön alaan kuuluvat määräykset ovat lakina voimassa. Vuoden 1994 sopimuksen osalta on kyse lainsäädännön alaan kuuluvien määräysten jälkikäteisestä voimaansaattamisesta. Määräyksiä on selostettu tarkemmin yksityiskohtaisissa perusteluissa sekä jäljempänä eduskunnan suostumuksen tarpeellisuutta koskevassa jaksossa.

2 §. Sopimuksen ja järjestelyn muiden määräysten voimaansaattamisesta sekä lain voimaantulosta säädettäisiin valtioneuvoston asetuksella.

4 Voimaantulo

Suomen ja Naton välinen järjestely tulee sen 16 artiklan 1 kohdan mukaisesti voimaan sinä päivänä, jonka Suomi ilmoittaa Natolle sen jälkeen, kun Suomi on saattanut kansalliset hyväksymistoimensa loppuun. Koska järjestely edellyttää voimaantullakseen Suomessa eduskunnan suostumusta ja tasavallan presidentin hyväksyntää perustuslain 8 luvun säännösten mukaisesti, tarkoituksena on, että Natolle ilmoitetaan järjestelyn voimaantulopäiväksi tietty päivä vasta kyseisten päätösten jälkeen. Päivämäärä on tarkoitus ajoittaa siten, että jäisi riittävästi aikaa järjestelyn ja lain voimaansaattamiseksi valtioneuvoston asetuksella. Laki on tarkoitettu tulemaan voimaan valtioneuvoston asetuksella säädettävänä ajankohtana samaan aikaan kuin järjestely tulee Suomen osalta voimaan. Lailla saatetaan samanaikaisesti voimaan myös vuoden 1994 Suomen ja Naton välisen tietoturvallisuussopimuksen lainsäädännön alaan kuuluvat määräykset.

5 Eduskunnan suostumuksen tarpeellisuus ja käsittelyjärjestys

5.1 Eduskunnan suostumuksen tarpeellisuus

Perustuslain 94 §:n 1 momentin mukaan eduskunta hyväksyy sellaiset valtiosopimukset ja muut kansainväliset velvoitteet, jotka sisältävät lainsäädännön alaan kuuluvia määräyksiä. Perustuslakivaliokunnan tulkintakäytännön mukaan määräys on luettava lainsäädännön alaan kuuluvaksi, jos se koskee jonkin perustuslaissa turvatun perusoikeuden käyttämistä tai rajoittamista, jos määräys muutoin koskee yksilön oikeuksien ja velvollisuuksien perusteita, jos määräyksen tarkoittamasta asiasta on perustuslain mukaan säädettävä lailla tai jos määräyksessä tarkoitetusta asiasta on jo voimassa lain säännöksiä taikka siitä on Suomessa vallitsevan käsityksen mukaan säädettävä lailla. Perustuslakivaliokunnan mukaan kansainvälisen velvoitteen määräys kuuluu näiden perusteiden mukaan lainsäädännön alaan siitä riippumatta, onko määräys ristiriidassa vai sopusoinnussa Suomessa lailla annetun säännöksen kanssa (kts. esimerkiksi PeVL 11/2000 vp ja PeVL 12/2000 vp).

Suomen ja Naton välinen järjestely turvallisuusluokitellun tiedon suojaamisesta

Järjestelyn 3 artiklassa määritellään, mitä tarkoitetaan turvallisuusluokitellulla tiedolla. Koska määritelmä vaikuttaa joko suoraan tai välillisesti sopimuksen lainsäädännön alaan kuuluvien aineellisten määräysten tulkintaan ja soveltamiseen, se edellyttää eduskunnan hyväksymistä (PeVL 6/2001 vp).

Järjestelyn 4 artiklassa on määräykset turvallisuusluokitusten merkitsemisestä ja niiden keskinäisestä vastaavuudesta. Yleisesti sovellettavat säännökset salassapito- ja luokitusmerkinnästä on säädetty julkisuuslain 25 §:ssä. Lain 25 §:n mukaan salassa pidettävään viranomaisen asiakirjaan on tehtävä merkintä asiakirjan salassa pitämisestä, kun tällainen asiakirja annetaan asianosaiselle ja kun asiakirja on pidettävä salassa toisen tai yleisen edun vuoksi. Muihin salaisiin asiakirjoihin tehtävä merkintä on harkinnanvarainen. 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. Määräykset kuuluvat lainsäädännön alaan.

Järjestelyn 5 artiklassa määrätään sopimuksen soveltamisalan piiriin kuuluvan turvallisuusluokitellun tiedon suojaamiseksi tarvittavista toimenpiteistä, jotka rajoittavat turvallisuusluokitellun tiedon luovuttamista sekä sen välittämistä, käyttämistä ja pääsyä siihen. Artiklassa on kyse järjestelyn ydinmääräyksestä, jonka perusteella Suomi voi suojata järjestelyn 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 kansainvälisestä tietoturvallisuusvelvoitteesta muuta johdu. Määräys kuuluu siten lainsäädännön alaan ja edellyttää eduskunnan suostumusta.

Järjestelyn 5 artiklan 1.2 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. Määräys kuuluu näin ollen lainsäädännön alaan.

Järjestelyn 6 artiklassa on ilmaistu turvallisuusluokiteltua tietoa saavia henkilöitä koskeva rajoitus. Artiklassa määrätään osapuolten velvollisuudesta teettää asianmukainen turvallisuusselvitys henkilöistä, joilla on tai saattaa olla pääsy sopimuksessa tarkoitettuun turvallisuusluokiteltuun tietoon. Turvallisuusselvitysten laadinnassa on otettava huomioon perustuslain 10 §:n 1 momentissa säädetty yksityiselämän suoja ja velvollisuus säätää henkilötietojen suojasta lailla. Suomessa turvallisuusselvityksen kohteena olevista henkilöistä sekä selvityksessä sovellettavasta menettelystä on säädetty turvallisuusselvityksistä annetussa laissa.

Järjestelyn 8 artiklassa todetaan, että järjestely ei vaikuta kummankaan osapuolen olemassaoleviin tai tuleviin immateriaalioikeuksiin (mukaan lukien patentit ja tekijänoikeudet), jotka liittyvät turvallisuusluokiteltuun tietoon. Kyse on toteavasta määräyksestä, jolla ei ole tarkoitus luoda uusia oikeuksia eikä velvollisuuksia, eikä sen siten voida katsoa kuuluvan lainsäädännön alaan. Tästä syystä määräykselle ei ole tarpeen hankkia myöskään eduskunnan suostumusta.

Osapuolten turvallisuusviranomaisten vierailuihin liittyy järjestelyn 12 artikla, joka mahdollistaa osapuolten toimivaltaisten turvallisuusviranomaisten vierailut toistensa luona. Osapuolten edustajien vierailuiden tarkoituksena on varmistaa sopimuksen tarkoituksen toteuttaminen turvallisuusluokiteltujen tietojen asianmukaiseksi suojaamiseksi. Tähän vierailuoikeuteen ei sisälly sellaista julkista vallan käyttöä ja tarkastusoikeutta, joka olisi ristiriidassa perustuslain kanssa (PeVL 39/1997 vp). Kansainvälisistä tieto-

turvallisuusvelvoitteista annetun lain 18 §:ssä on vastaavat säännökset vierailuja koskevan sopimusmääräyksen täytäntöönpanoon liittyvistä seikoista. Määräykset kuuluvat lainsäädännön alaan.

Järjestelyn 13 artiklassa edellytetään, että kumpikin osapuoli ilmoittaa viipymättä toiselle osapuolelle todetusta tai epäillystä turvallisuusluokitellun tiedon katoamisesta tai vaarantumisesta. Vastaanottavan osapuolen on lisäksi toteutettava kaikki asianmukaiset toimenpiteet loukkauksen tutkimiseksi ja korjaamiseksi. Tuloksista on ilmoitettava viipymättä toiselle osapuolelle. Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 19 §:ssä säädetään kansalliselle turvallisuusviranomaiselle kuuluvista velvoitteista sopimusmääräyksissä tarkoitetuissa tilanteissa. Artiklan määräykset kuuluvat näin ollen lainsäädännön alaan.

Suomen ja Naton välinen vuoden 1994 tietoturvallisuussopimus

Sopimuksen 1 artikla sisältää järjestelyä vastaavat periaatteet turvallisuusluokitellun tiedon vastavuoroisesta suojaamisesta. Sopimuksen 2 artikla koskee velvollisuutta tehdä henkilöstöturvallisuusselvitykset. Kyseisten määräysten on katsottava kuuluvan lainsäädännön alaan samoin perustein kuin edellä on selvitetty järjestelyn 5 ja 6 artiklan yhteydessä.

5.2 Käsittelyjärjestys

Suomen hallituksen ja Naton välillä tietoturvallisuussopimus arvioitiin valtioneuvostossa sen hyväksymishetkellä voimassa olleen valtiosäännön mukaisesti niin sanotuksi kansainväliseksi hallintosopimukseksi ja se hyväksyttiin ulkoasiainministeriön päätöksellä 13 päivänä syyskuuta 1994 allekirjoitusvaltuuksien myöntämisen yhteydessä.

Perustuslain 94 §:ssä on kyse tosiasiallisesti siitä, että eduskunta hyväksyessään valtiosopimuksen tai muun kansainvälisen velvoitteen antaa suostumuksensa sille, että tasavallan presidentti tai valtioneuvosto päättää velvoitteeseen sitoutumisesta. Vuoden 1994 sopimus on aikanaan kansallisesti hyväksytty hyväksymishetkellä voimassa olleen valtiosäännön mukaisesti ja sitä on allekirjoitushetkestä tosiasiallisesti sovellettu Suomen ja Naton välillä. Sopimus on näin ollen Suomea sitova perustuslaissa tarkoitettu kansainvälinen velvoite. Kansainvälisen velvoitteen voimaansaattamisessa on sen sijaan kyse valtionsisäisestä toimenpiteestä, joka voidaan toteuttaa myös jälkikäteen. Tämän johdosta sopimusta ei esitetä perustuslain 94 §:n perusteella eduskunnan hyväksyttäväksi, vaan se esitetään voimaansaatettavaksi blankettisäännöksellä, joka on sisällytetty Suomen ja Naton välistä järjestelyä koskevaan voimaansaattamislakiin.

Lainsäädännön alaa koskevan käsityksen muuttuessa uuden perustuslain ja sitä koskevan tulkintakäytännön myötä aiemmin asetuksella voimaansaatettujen sopimusten voimaansaattamissäädöksiä ei ole ryhdytty korottamaan lain tasolle, ellei siihen ole erityisiä syitä. Vastaavasti aikanaan kansainvälisinä hallintosopimuksina käsiteltyjä sopimuksia ei saateta myöhemmin voimaan lain tasolla ilman erityistä syytä. Erityinen peruste vuoden 1994 sopimuksen voimaansaattamiselle on tarve soveltaa sopimukseen ja vuonna 2012 tehtyyn järjestelyyn Suomen kansainvälisistä tietoturvallisuusvelvoitteista annettua lakia. Toisin kuin pakolaisten oikeusasemaa koskevan yleissopimuksen kohdalla (ks. HE 32/2004 vp) kysymyksessä olisi varsinainen voimaansaattamissäännös, koska sopimusta ei ole aiemmin saatettu voimaan alemmantasoisella säädöksellä.

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 tarvit-

sevat 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 järjestelyn 5 artiklan määräykset eivät laajenna salassapitovelvollisuutta siitä, mitä salassapidosta on säädetty sanotun lain 6 §:ssä. Määräykset eivät siten vaikuta sopimuksen käsittelyjärjestykseen.

Hallinnolliseen järjestelyyn Suomen ja Naton kesken vaihdettavan turvallisuusluokitellun tiedon suojaamisesta ei voida katsoa sisältyvän sellaisia määräyksiä, jotka koskisivat perustuslakia sen 94 §:n 2 momentissa ja 95 §:n 2 momentissa tarkoitetulla tavalla. Hallituksen näkemyksen mukaan järjestely voitaisiin näin ollen hyväksyä äänten enemmistöllä ja ehdotus sen lainsäädännön alaan kuuluvien sopimusmääräysten voimaansaattamiseksi tavallisen lain säätämisjärjestyksessä.

Suomen ja Naton välisen vuoden 1994 tietoturvallisuussopimuksen määräykset, jotka edellä esitetyn mukaisesti esitetään saatettavaksi voimaan lailla, eivät myöskään koske perustuslakia.

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

eduskunta hyväksyisi Suomen ja Pohjois-Atlantin liiton kesken vaihdettavan turvallisuusluokitellun tiedon suojaamisesta Helsingissä 3 päivänä heinäkuuta 2012 tehdyn hallinnollisen järjestelyn.

Eduskunnan hyväksyttäväksi annetaan samalla seuraava lakiehdotus:

Lakiehdotus

Laki

Suomen ja Pohjois-Atlantin liiton kesken vaihdettavan turvallisuusluokitellun tiedon suojaamisesta tehdyn hallinnollisen järjestelyn ja Pohjois-Atlantin liiton kanssa tehdyn tietoturvallisuussopimuksen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta

Eduskunnan päätöksen mukaisesti säädetään:

1 §

Suomen ja Pohjois-Atlantin liiton kesken vaihdettavan turvallisuusluokitellun tiedon suojaamisesta Helsingissä 3 päivänä heinäkuuta 2012 tehdyn hallinnollisen järjestelyn sekä Suomen ja Pohjois-Atlantin liiton välillä Brysselissä 22 päivänä syyskuuta 1994 tehdyn tietoturvallisuussopimuksen lainsäädännön alaan kuuluvat määräykset ovat lakina voimassa sellaisina kuin Suomi on niihin sitoutunut.

2 §

Järjestelyn ja sopimuksen muiden määräysten voimaansaattamisesta ja tämän lain voimaantulosta säädetään valtioneuvoston asetuksella.

Helsingissä 25 päivänä lokakuuta 2012

Pääministeri

JYRKI KATAINEN

Lainsäädäntöneuvos *Kaija Suvanto*

Sopimustekstit

(käännös)

HALLINNOLLINEN JÄRJESTELY SUOMEN TASAVALLAN HALLITUKSEN JA POHJOIS-ATLANTIN LIITON KESKEN VAIHDETTAVAN TURVALLISUUSLUOKITELLUN TIEDON SUOJAAMISEKSI

ADMINISTRATIVE ARRANGEMENT FOR THE PROTECTION OF CLASSIFIED INFORMATION EXCHANGED BETWEEN THE GOVERNMENT OF THE REPUBLIC OF FINLAND AND THE NORTH ATLANTIC TREATY ORGANISATION

1. JOHDANTO

Suomen tasavallan hallitus ja Pohjois-Atlantin liitto (Nato) (jäljempänä "osapuolet"), jotka ovat tehneet tietoturvallisuussopimuksen Suomen ja Pohjois-Atlantin liiton välillä ja toimivat tämän sopimuksen 4 artiklan mukaisesti, ovat tällä hallinnollisella järjestelyllä määränneet turvallisuuskäytännöistä ja -menettelyistä turvallisuusluokitellun tiedon suojaamiseksi.

1. INTRODUCTION

The Government of the Republic of Finland and theNorth Atlantic Treaty Organisation and (hereinafter referred to as "the Participants") having entered into the "*Security Agreement between Finland and the North Atlantic Treaty Organization*" and pursuant to Article 4 of that Agreement, have set out security practices and procedures for the protection of Classified Information in this Administrative Arrangement.

2. TURVALLISUUSVIRANOMAISET

2.1 Osapuolten turvallisuusviranomaiset vastaavat tästä täytäntöönpanojärjestelystä. Osapuolten turvallisuusviranomaiset ovat

2.1.1 Pohjois-Atlantin liiton osalta

NATO Office of Security (NOS, Naton turvallisuustoimisto)
NATO HQ
Boulevard Leopold III
B-1110 Brussels
BELGIUM

2.1.2 Suomen tasavallan hallituksen osalta

Kansallinen turvallisuusviranomainen (National Security Authority, NSA).

2.2 Osapuolet toimittavat toisilleen edellä mainittuja viranomaisia koskevat tiedot.

2. SECURITY AUTHORITIES

2.1 The Security Authorities of the Participants will be responsible for this Administrative Arrangement. The Security Authorities for the Participants will be:

2.1.1 For the North Atlantic Treaty Organisation
NATO Office of Security

NATO HQ
Boulevard Leopold III
B-1110 Brussels
BELGIUM

2.1.2 For the Government of the Republic of Finland
National Security Authority (NSA)

2.2 Details about the above authorities will be exchanged by the Participants.

3. MÄÄRITELMÄT

3.1 Tässä järjestelyssä sovelletaan seuraavia määritelmiä:
3.1.1 “turvallisuusluokiteltu tieto” tarkoittaa kaikkea jommaltakummalta osapuolelta peräisin olevaa tai jommankumman osapuolen tuottamaa tai vaihtamaa tietoa ja aineistoa, johon sovelletaan turvallisuusluokitusta (mukaan lukien asiakirjat, laitteet, aineet ja muut esineet kaikissa muodoissaan sekä kaikki tällaisen tiedon tai aineiston jäljennökset ja käännökset), riippumatta siitä, välitetäänkö tämä tieto tai aineisto suullisesti, kuvallisesti, kirjallisesti vai muussa muodossa vai muulla tavalla;
3.1.2 “luovuttava osapuoli” tarkoittaa tiedon luovuttavaa osapuolta;
3.1.3 “välittävä osapuoli” tarkoittaa tiedon välittävää osapuolta;
3.1.4 “vastaanottava osapuoli” tarkoittaa osapuolta, joka saa tiedon välittävältä osapuolelta;
3.1.5 “kolmas osapuoli” tarkoittaa muuta henkilöä tai yhteisöä kuin osapuolia.

4. TURVALLISUUSLUOKITELLUN TIEDON MERKITSEMINEN

4.1 Luovuttava osapuoli merkitsee kaikkeen turvallisuusluokiteltuun tietoon asianmukaisen 4.3 kohdassa mainitun turvallisuusluokan. Jos merkinnän tekeminen on käytännössä mahdotonta, luovuttava osapuoli ilmoittaa luokan erikseen vastaanottavalle osapuolelle.

4.2 Luovuttavan osapuolen vastaanottavalle osapuolelle luovuttaman turvallisuusluokitellun tiedon omistajuus, leima ja turvallisuusluokka säilyvät muuttumattomina.
4.3 Osapuolten turvallisuusluokat vastaavat toisiaan seuraavasti:

3. DEFINITIONS

3.1 For the purpose of this Arrangement the following definitions will apply:
3.1.1 “Classified Information” means all information and material originated, generated or exchanged by either Participant (including documents, equipment, substances and other items in any form or any reproduction or translation of such information or material) which is subject to a security classification, regardless of whether it is provided orally, visually, in writing, or in any other form or manner;

3.1.2 “Originating Participant” means that Participant which owns the information;
3.1.3 “Transmitting Participant” means that Participant which transmits the information;
3.1.4 “Receiving Participant” means that Participant which receives information from the Transmitting Participant;
3.1.5 “Third Participant” means any person or entity other than the Participants;

4. MARKING OF CLASSIFIED INFORMATION

4.1 The Originating Participant will mark all Classified Information with the appropriate security classification as specified in Paragraph 4.3. Where marking is not physically possible the Originating Participant will advise the Receiving Participant of the classification separately.

4.2 Classified Information released by the Originating Participant to the Receiving Participant will retain its ownership, label and security classification.
4.3 The corresponding security classifications of the Participants are as follows:

Naton osalta/For NATO	Suomen osalta/For Finland
NATO SECRET	SALAINEN or HEMLIG

NATO CONFIDENTIAL	LUOTTAMUKSELLINEN or KONFIDENTIELL
NATO RESTRICTED	KÄYTTÖ RAJOITETTU or BEGRÄNSAD TILLGÅNG

4.4 Osapuolen tuottamaan turvallisuusluokiteltuun tietoon, joka sisältää myös toisen osapuolen antamaa turvallisuusluokiteltua tietoa, merkitään etuliitteeksi SUOMI/NATO tai NATO/SUOMI ja sen jälkeen asianmukainen turvallisuusluokka, jotta asiakirjan voidaan todeta sisältävän yhteisesti omistettua turvallisuusluokiteltua tietoa.

4.4 Classified Information produced by one Participant that also contains Classified Information provided by the other Participant will be prefixed FINLAND/NATO or NATO/FINLAND followed by the appropriate security classification so as to identify that the document contains jointly owned Classified Information.

5. TURVALLISUUSLUOKITELLUN TIEDON SUOJAAMINEN JA KÄYTTÖ

5. PROTECTION AND USE OF CLASSIFIED INFORMATION

5.1. Osapuolet soveltavat turvallisuusluokitellun tiedon suojaamiseen ja käyttöön seuraavia määräyksiä:

5.1.1 vastaanottava osapuoli antaa kaikelle turvallisuusluokitellulle tiedolle vähintään samantasoisen fyysisen ja oikeudellisen suojan kuin omalle vastaavaan turvallisuusluokkaan kuuluvalle tiedolleen;

5.1.2 vastaanottava osapuoli ei salli turvallisuusluokitellun tiedon käyttämistä muuhun kuin siihen tarkoitukseen, jota varten se annetaan, ilman luovuttavan osapuolen kirjallista ennakkosuostumusta;

5.1.3 ennen kuin kolmannelle osapuolelle paljastetaan ja luovutetaan tämän järjestelyn mukaisesti saatua turvallisuusluokiteltua tietoa tai sille annetaan pääsy tällaiseen tietoon, asiaan on saatava luovuttavan osapuolen kirjallinen ennakkosuostumus;

5.1.4 vastaanottava osapuoli noudattaa niitä lisärajoituksia, joita luovuttava osapuoli tai joku muu tämän puolesta voi asettaa turvallisuusluokitellun tiedon käyttämiselle, paljastamiselle ja luovuttamiselle sekä pääsylle tähän tietoon;

5.1.5 vastaanottava osapuoli ei alenna luovuttavan osapuolen antamaa turvallisuusluokkaa vastaavaa turvallisuusluokkaa ilman luovuttavan osapuolen kirjallista ennak-

5.1. The Participants will apply the following rules for the protection and use of Classified Information:

5.1.1 the Receiving Participant will accord to all Classified Information a standard of physical and legal protection no less stringent than that which it provides to its own information of corresponding classification;

5.1.2 the Receiving Participant will not permit Classified Information to be used for any purpose other than that for which it is provided, without the prior written approval of the Originating Participant;

5.1.3 the written consent of the Originating Participant must be obtained prior to the disclosure and release to, or access by, any Third Participant of any Classified Information obtained under this Arrangement;

5.1.4 the Receiving Participant will comply with any additional limitations on the use, disclosure, release and access to Classified Information which may be specified by, or on behalf of, the Originating Participant;

5.1.5 the Receiving Participant will not downgrade the security classification corresponding to the classification assigned by the Originating Participant without the prior

kosuostumusta;

5.1.6 luovuttava osapuoli ilmoittaa vastaanottavalle osapuolelle turvallisuusluokitellun tiedon turvallisuusluokan muuttumisesta (esimerkiksi luokan alentamisesta tai tiedon uudelleenluokittelusta); ja

5.1.7 vastaanottava osapuoli toteuttaa kaikki tarvittavat toimet suojatakseen turvallisuusluokiteltua tietoa luvattomalta paljastamiselta.

5.2 Kumpikin osapuoli on tietoinen kummankin osapuolen vähimmäisvaatimuksista, jotka koskevat turvallisuusluokitellun tiedon käsittelyä. Naton osalta nämä vaatimukset esitetään asiakirjassa C-M(2002)49, "Security within the North Atlantic Treaty Organisation", ja sitä tukevissa ohjeissa, erityisesti ohjeessa AC/35-D/1038, "Supporting Document on the Security Protection of NATO Information Released to Non-NATO Nations and International Organisations". Suomen osalta nämä vaatimukset esitetään asiaa koskevissa Suomen säädöksissä ja määräyksissä.

5.3 Kun tietoa ei enää tarvita siihen tarkoitukseen, jota varten se on annettu, vastaanottava osapuoli joko palauttaa tiedon luovuttavalle osapuolelle siten kuin nämä osapuolet keskenään sopivat tai hävittää tiedon vastaanottavan osapuolen menettelyjä noudattaen.

5.4. Osapuolet voivat keskenään päättää asianmukaisiksi katsomistaan lisävaatimuksista, jotka koskevat turvallisuusluokitellun tiedon suojaamista.

5.5 Luovuttava osapuoli pidättää itsellään oikeuden kieltäytyä välittämästä turvallisuusluokiteltua tietoaan.

6. PÄÄSY TURVALLISUUSLUOKITELTUUN TIETOON

6.1 Jollei luovuttava osapuoli ole toisin määrännyt, pääsy turvallisuusluokiteltuun tietoon sallitaan sellaisille Suomen kansalaisille ja Naton virkamiehille,

6.1.2 joilla on todistus asianmukaisen tason turvallisuusselvityksestä;

6.1.3 jotka tarvitsevat tietoa työtehtäviensä suorittamiseen (tiedonsaantitarpeen periaate); ja

6.1.4 joille on selostettu noudatettavat turvallisuusmenettelyt.

written approval of the Originating Participant;

5.1.6 the Originating Participant will inform the Receiving Participant of any change in the classification of Classified Information (e.g. downgrading or reclassification); and

5.1.7 the Receiving Participant will take all the necessary steps to protect Classified Information from unauthorised disclosure.

5.2 Both Participants are aware of the minimum standards for the handling of Classified Information for each Participant. For NATO these are outlined in C-M(2002)49, "Security within the North Atlantic Treaty Organisation" and its supporting Directives, in particular AC/35-D/1038, the "Supporting Document on the Security Protection of NATO Information Released to Non-NATO Nations and International Organisations". For Finland these are outlined in relevant Finnish laws and regulations.

5.3 When information is no longer required for the purpose for which it was provided, the Receiving Participant will either return the information to the Originating Participant as mutually arranged between them or destroy the information in accordance with the procedures of the Receiving Participant.

5.4. The Participants may mutually determine any additional requirements for security protection of Classified Information as they consider appropriate.

5.5 The Originating Participant reserves the right to refuse to transmit any of its Classified Information.

6. ACCESS TO CLASSIFIED INFORMATION

6.1 Unless the Originating Participant has stated otherwise, access to Classified Information will be granted to citizens of Finland and officials of NATO who:

6.1.2 have been given a security clearance to the appropriate level;

6.1.3 require the information for the performance of their official duties (the need-to-know principle); and

6.1.4 have been briefed on the respective

vallisuusmenettelyt ja jotka ovat tunnustaneet turvallisuusvelvoitteensa.

7. TURVALLISUUSLUOKITELLUN TIEDON VÄLITTÄMINEN

7.1 Osapuolet välittävät turvallisuusluokitellun tiedon toisilleen välittävän osapuolen turvallisuusmääräysten ja -menettelyjen mukaisesti.

7.2 Jolleivät osapuolet keskenään toisin päätä, turvallisuusluokiteltu tieto välitetään Suomen tai Naton virallisia kanavia käyttäen.

7.3 Osapuolet voivat välittää turvallisuusluokiteltua tietoa sähköisesti. Tätä varten Naton turvallisuustoimisto ja Suomen kansallinen tietoturvaviranomainen luovat keskenään erityiset menettelyt.

8. IMMATERIAALIOIKEUDET

Mikään tämän hallinnollisen järjestelyn määräys ei vähennä tai rajoita kummankaan osapuolen olemassa olevia tai myöhemmin saatavia immateriaalioikeuksia (mukaan lukien patentit ja tekijänoikeudet), jotka liittyvät turvallisuusluokiteltuun tietoon.

9. TURVALLISUUSVAATIMUSTEN YKSITYISKOHDAT

Osapuolet antavat toisilleen tiedot turvallisuusluokitellun tiedon suojaamista koskevista turvallisuusvaatimuksistaan, -käytännöistään ja -menettelyistään. Osapuolet ilmoittavat toisilleen kirjallisesti turvallisuusvaatimustensa, -käytäntöjensä ja -menettelyjensä muutoksista, jotka vaikuttavat siihen, miten turvallisuusluokiteltua tietoa suojataan.

10. JÄRJESTELYN NOUDATTAMINEN JA TURVALLISUUSTARKASTUKSET

10.1 Kumpikin osapuoli vastaa sen varmistamisesta, että sen laitokset, organisaatiot ja henkilöstö noudattavat tätä hallinnollista järjestelyä.

10.2 Osapuolet suorittavat tarvittavat tur-

security procedures and have acknowledged their security obligations.

7. TRANSMISSION OF CLASSIFIED INFORMATION

7.1 Classified Information will be transmitted between the Participants in accordance with the security regulations and procedures of the Transmitting Participant.

7.2 Unless otherwise mutually determined by the Participants, Classified Information will be transmitted through official Finnish or NATO channels.

7.3 The Participants may transmit Classified Information by electronic means. To this end specific procedures will be established between the NOS and Finnish NCSA.

8. INTELLECTUAL PROPERTY

Nothing in this Administrative Arrangement diminishes or limits any existing or acquired intellectual property rights (including patents and copyrights) associated with Classified Information to which either Participant may be entitled.

9. DETAILS OF SECURITY STANDARDS

Each Participant will provide to the other information about its security standards, practices and procedures for the safeguarding of Classified Information. Each Participant will inform the other Participant in writing of any changes to its security standards, procedures, and practices which have an effect on the manner in which Classified Information is protected.

10. COMPLIANCE AND SECURITY INSPECTIONS

10.1 Each Participant will be responsible for ensuring compliance by its establishments, facilities and personnel of this Administrative Arrangement.

10.2 Each Participant will conduct the nec-

vallisuustarkastukset varmistaakseen, että asianmukaisia turvallisuusmääräyksiä ja -menettelyjä noudatetaan.

11. VIERAILUT – YLEISTÄ

11.1 Vierailut, jotka edellyttävät pääsyä turvallisuusluokiteltuun tietoon tai turvallisuusselvitystä edellyttävään laitokseen, sallitaan ainoastaan sellaisille henkilöille, joilla on voimassa oleva todistus asianmukaisen tason turvallisuusselvityksestä ja jotka tarvitsevat pääsyä kyseiseen tietoon tai laitokseen suorittaakseen työtehtäviään.

11.2 Vierailevan osapuolen toimivaltainen turvallisuuselin, jonka asianomainen turvallisuusviranomainen nimeää, toimittaa vierailupyynnöt hyväksyttäväksi isäntänä toimivan osapuolen toimivaltaiselle turvallisuuselimelle, jonka asianomainen turvallisuusviranomainen nimeää, vähintään kaksikymmentä (20) työpäivää ennen ehdotetun vierailun ajankohtaa.

11.3 Näissä hyväksyntäpyynnöissä annetaan seuraavat tiedot:

11.3.1 ehdotetun vierailun tarkoitus;

11.3.2 vierailun ehdotettu ajankohta ja kesto;

11.3.3 yksityiskohtaiset tiedot vierailun kohteena olevista laitoksista, organisaatioista ja henkilöstöstä;

11.3.4 sen vierailevan osapuolen virkamiehen henkilötiedot ja puhelinnumero, joka voi antaa lisätietoja vierailusta;

11.3.5 mahdollisuuksien mukaan vierailun kohteena olevien laitosten, toimitilojen ja organisaatioiden yhteyshenkilöiden henkilötiedot ja puhelinnumerot;

11.3.6 vierailuun liittyvän turvallisuusluokitellun tiedon arvioitu taso; ja

11.3.7 seuraavat tiedot vierailijoista:

11.3.7.1 koko nimi;

11.3.7.2 syntymäaika ja -paikka;

11.3.7.3 kansalaisuus ja passin numero;

11.3.7.4 vierailijoiden edustama virasto, yritys tai organisaatio, heidän nykyinen tehtävänsä ja tarvittaessa arvoasemansa; ja

11.3.7.5 kunkin vierailijan todistus henkilöturvallisuusselvityksestä, sen antamispäivä,

essary security inspections to ensure the appropriate security regulations and procedures are complied with.

11. VISITS - GENERAL

11.1 Approval for visits requiring access to Classified Information or access to an establishment requiring a security clearance, will be granted only to personnel who possess a valid security clearance to the appropriate level and require such access for the performance of their official duties.

11.2 Requests for visits will be submitted for approval by the appropriate security body of the visiting Participant, as identified by the Security Authority, to the appropriate security body of the host Participant, as identified by the Security Authority, not less than twenty (20) working days prior to the date of the proposed visit.

11.3 Such requests for approval will specify:

11.3.1 the purpose of the proposed visit;

11.3.2 the proposed date and duration of the visit;

11.3.3 particulars of the establishments, facilities and organisations to be visited;

11.3.4 the identification and telephone number of an official of the visiting Participant who can provide additional information concerning the visit;

11.3.5 if possible, the identification and telephone number of contacts at the establishments, facilities and organisations to be visited;

11.3.6 the anticipated level of Classified Information to be involved; and

11.3.7 the following details of the personnel who will undertake the visit:

11.3.7.1 full name;

11.3.7.2 date and place of birth;

11.3.7.3 citizenship and passport number;

11.3.7.4 agency, company or organisation represented, present position and, if appropriate, rank; and

11.3.7.5 the personnel security clearance held, the date of its issue, the period of its va-

voimassaoloaika ja mahdolliset rajoitukset.

11.4 Vierailupyyntöjen tueksi toimitetaan todistukset kunkin vierailijan turvallisuusselvityksen tasosta.

11.5 Kaikki vierailijat noudattavat asianmukaisia turvallisuusmääräyksiä ja isäntänä toimivan osapuolen sovellettavia laitoskohtaisia ohjeita.

11.6 Mikään tämän artiklan määräys ei rajoita kummankaan osapuolen oikeutta sallia toisen osapuolen vierailijoiden pääsy turvallisuusluokiteltuun tietoon tai kulku valvotuille alueille tai muihin laitoksiin milloin tahansa hyväksytyn vierailun aikana, jos isäntänä toimiva osapuoli haluaa sallia tällaisen pääsyn tai kulun.

12. TARKASTUSVIERAILUT

Tarkastaakseen, että turvallisuusluokiteltua tietoa säilytetään ja käsitellään keskinäisesti päätettyjen vähimmäisvaatimusten mukaisesti, Naton turvallisuustoimisto ja Suomen kansallinen turvallisuusviranomainen päättävät keskenään tämän järjestelyn 11 artiklan mukaisesti järjestettävistä vastavuoroisista vierailuista ja suorittavat niitä.

13. KATOAMINEN TAI VAARANTUMINEN

13.1 Jos turvallisuusluokiteltua tietoa katoaa tai vaarantuu tai sen epäillään kadonneen tai vaarantuneen, vastaanottava osapuoli ilmoittaa asiasta välittömästi luovuttavalle osapuolelle ja/tai välittävälle osapuolelle.

13.2 Vastaanottava osapuoli tutkii välittömästi tällaisen katoamisen tai vaarantumisen ja ilmoittaa luovuttavalle osapuolelle ja/tai välittävälle osapuolelle viipymättä tutkinnan tuloksista ja toteutetuista tai toteutettavista korjaustoimista.

14. KUSTANNUKSET

Osapuolet vastaavat omista kustannuksistaan, jotka niille aiheutuvat tämän hallinnollisen järjestelyn täytäntöönpanosta.

lidity and any limitations.

11.4 Visit requests will be supported by a certification of the level to which each visitor has been security cleared.

11.5 All visitors will comply with the appropriate security regulations and relevant establishment instructions of the host Participant.

11.6 Nothing in this Section will restrict the right of either Participant to permit visiting personnel of the other Participant to have access to Classified Information or entry to controlled areas or any other establishments at any time during an approved visit should the host Participant wish to grant such access or entry.

12. VERIFICATION VISITS

Reciprocal visits, arranged in accordance with Section 11 of this Arrangement, will be mutually determined and conducted by the NATO Office of Security and the National Security Authority of Finland to verify that Classified Information is being stored and handled in accordance with mutually determined minimum standards.

13. LOSS OR COMPROMISE

13.1 In the event of loss or compromise or suspected loss or compromise of Classified Information, the Receiving Participant will immediately inform the Originating Participant and/or Transmitting Participant.

13.2 The Receiving Participant will immediately investigate such loss or compromise and will, without delay, inform the Originating Participant and/or Transmitting Participant of the circumstances, the findings of the investigation and corrective action taken or to be taken.

14. COSTS

Each Participant will be responsible for its own costs incurred in implementing this Administrative Arrangement.

15. RIITOJEN RATKAISEMINEN

Riidat, jotka koskevat tämän hallinnollisen järjestelyn tulkintaa tai soveltamista, ratkaistaan osapuolten välisin kuulemisin ja neuvotteluin, eikä niitä saateta kansallisten tai kansainvälisten tuomioistuinten tai kolmansien osapuolten ratkaistaviksi.

15. SETTLEMENT OF DISPUTES

Disputes arising from the interpretation or application of this Administrative Arrangement will be settled by consultation and negotiation between the Participants and will not be referred to any national or international tribunal or any Third Participant.

16. JÄRJESTELYN VOIMAANTULO, UUDELLEENTARKASTELU, MUUTTAMINEN, KESTO JA PÄÄTTYMINEN

16. 1 Suomi ilmoittaa Natolle, kun kansalliset hyväksymistoimet on suoritettu. Hallinnollinen järjestely tulee voimaan Suomen ilmoittamana päivänä.

16.2 Järjestelyä ja sen soveltuvuutta voidaan tarkastella uudelleen jommankumman osapuolen pyynnöstä, ja sitä voidaan muuttaa osapuolten keskinäisellä kirjallisella suostumuksella.

16.3 Järjestelyn päättymisen estämättä jatketaan niiden voimassa olevien vastuiden ja velvoitteiden soveltamista, jotka liittyvät välitetyn turvallisuusluokitellun tiedon suojaamiseen ja käyttöön.

16. ENTRY INTO FORCE, REVIEW, AMENDMENT, DURATION AND TERMINATION

16. 1 Finland will notify the NATO of the completion of the internal approval measures. The Arrangement will enter into force on the date to be communicated by Finland.

16.2 The Administrative Arrangement and its applicability may be reviewed at the request of either Participant and amended by mutual written consent of the Participants.

16.3 The existing responsibilities and obligations relating to the protection and use of Transmitted Classified Information will continue to apply notwithstanding the termination of this Arrangement.

Suomen hallitus ja Pohjois-Atlantin liitto ovat allekirjoittaneet tämän järjestelyn.

Helsingissä 3 päivänä heinäkuuta 2012 kahtena englanninkielisenä kappaleena.

The Government of Finland and the NATO have signed this Arrangement

in Helsinki on the 3rd day of July 2012 in two originals in the English language.

Suomen tasavallan hallituksen puolesta

Charles Murto
Suomen kansallinen turvallisuusviranomaisen päällikkö

For the Government of the Republic of Finland

Charles Murto
Director, National Security Authority of Finland

Pohjois-Atlantin liiton puolesta

Stephen F. Smith
johtaja, Naton turvallisuustoimisto

For the NATO

Stephen F. Smith
Director, Nato Office of Security

(käännös)

TIETOTURVALLISUUSSOPIMUS SUOMEN JA POHJOIS-ATLANTIN LIITON VÄLILLÄ

TIETOTURVALLISUUSSOPIMUS

Suomen hallitus,
edustajanaan suurlähettiläs Olli Mennander, pysyvä yhteysvirkamies Pohjois-Atlantin liiton päämajassa,
ja
Pohjois-Atlantin liitto (Nato),
edustajanaan Pohjois-Atlantin liiton pääsihteerin sijainen Sergio Balanzino,

jotka

ottavat huomioon, että Suomi toimii Pohjois-Atlantin yhteistyöneuvoston/Naton rauhankumppanuuden kumppanivaltiona;
ovat sopineet neuvottelevansa keskenään poliittisista ja turvallisuuteen liittyvistä asioista sekä laajentavansa ja vahvistavansa poliittista ja sotilaallista yhteistyötä kaikkialla Euroopassa,
ymmärtävät, että tehokas yhteistyö näissä asioissa edellyttää arkaluonteisten ja/tai salassa pidettävien tietojen vaihtamista osapuolten kesken,

ovat sopineet seuraavasta:

1 artikla

Osapuolet
(i) suojaavat ja turvaavat toisen osapuolen tiedot ja aineistot;
(ii) pyrkivät kaikin keinoin varmistamaan, että jos tällaiset tiedot ja aineistot on turvallisuusluokiteltu, niillä säilytetään ne turvallisuusluokat, jotka jompikumpi osapuoli on määrännyt siltä peräisin oleville tiedoille ja aineistoille, sekä suojaavat tällaiset tiedot ja aineistot sovittuja yhteisiä vaatimuksia noudattaen;
(iii) eivät käytä vaihdettuja tietoja ja aineistoja muihin kuin niihin tarkoituksiin, joista

SECURITY AGREEMENT BETWEEN FINLAND AND THE NORTH ATLANTIC TREATY ORGANIZATION

SECURITY AGREEMENT

The Government of Finland
represented by His Excellency Mr. Olli MENNANDER, Ambassador, Permanent Liaison Officer to NATO Headquarters

The North Atlantic Treaty Organization
represented by Mr. Sergio BALANZINO
Acting Secretary General of the North Atlantic Treaty Organization

Considering that Finland is a Partner Country in the North Atlantic Cooperation Council (NACC) / Partnership for Peace (PfP);
Having agreed to consult on political and security-related issues and expand and intensify political and military cooperation throughout Europe;

Realizing that effective co-operation in these regards entails the exchange of sensitive and/or privileged information among the parties;

Have agreed as follows:

Article 1

The Parties will:
(i) protect and safeguard the information and material of the other Party;
(ii) make every effort to ensure that, if it is classified, such information and material will maintain the security classifications established by any Party with respect to information and material of that Party's origin and safeguard such information and material to agreed common standards;

(iii) not use the exchanged information and material for purposes other than those laid

on määrätty asianomaisissa ohjelmissa ja näitä ohjelmia koskevissa päätöksissä ja päätöslauselmissa;

(iv) eivät paljasta tällaisia tietoja ja aineistoja kolmansille osapuolille ilman luovuttajan suostumusta.

2 artikla

(i) Suomen hallitus hyväksyy sitoumuksen tehdä kaikista kansalaisistaan, jotka työtehtäviään suorittaessaan tarvitsevat pääsyä Pohjois-Atlantin yhteistyöneuvoston tai rauhankumppanuuden ohjelmien mukaisesti vaihdettaviin tietoihin tai aineistoihin tai saattavat päästä niihin, asianmukainen turvallisuusselvitys ennen kuin heille annetaan pääsy tällaisiin tietoihin ja aineistoihin.

(ii) Turvallisuusselvitysmenettelyt olisi suunniteltava sellaisiksi, että niissä määritetään, voidaanko henkilölle hänen lainkuuliaisuutensa ja luotettavuutensa huomioon ottaen sallia pääsy turvallisuusluokiteltuihin tietoihin vaarantamatta niiden turvallisuutta.

3 artikla

Naton turvallisuustoimisto, joka toimii pääsihteerin ja Naton sotilaskomitean puheenjohtajan johdolla ja puolesta, puheenjohtajan toimiessa Naton neuvoston ja Naton sotilaskomitean nimissä ja alaisuudessa, vastaa yhteistyöneuvosto- tai rauhankumppanuusyhteistyössä vaihdettavia turvallisuusluokiteltuja tietoja koskevista turvallisuusjärjestelyistä.

4 artikla

Suomen hallitus ilmoittaa Naton turvallisuustoimistolle turvallisuusviranomaisensa, jolla on vastaava kansallinen vastuu. Suomen hallituksen ja Naton välillä tehdään erilliset hallinnolliset järjestelyt, jotka koskevat muun muassa vaihdettavien tietojen vastavuoroisen suojaamisen vaatimuksia sekä Suomen turvallisuusviranomaisen ja Naton turvallisuustoimiston välisiä yhteyksiä.

down in the framework of the respective programmes and the decisions and resolutions pertaining to these programmes;

(iv) not disclose such information and material to third parties without the consent of the originator;

Article 2

(i) The Government of Finland accepts the commitment to have all persons of its nationality who, in the conduct of their official duties, require or may have access to information or material exchanged under the NACC or PfP programmes appropriately cleared before they are granted access to such information and material.

(ii) The security clearance procedures should be designed to determine whether an individual can, taking into account his loyalty and trustworthiness, have access to classified information without risk to its security.

Article 3

The NATO Office of Security (NOS), under the direction and on behalf of the Security General and the Chairman, NATO Military Committee, acting in the name of the North Atlantic Council and the NATO Military Committee and under their authority, is responsible for security arrangements for the protection of classified information exchanged within the NACC/PfP co-operation.

Article 4

The Government of Finland will inform the NOS of the security authority with the similar national responsibility. Separate Administrative Arrangements will be worked out between the Government of Finland and NATO which will cover i.a. the standards of the reciprocal security protection for the information to be exchanged and the liaison between the security authority of Finland and the NOS.

5 artikla

Ennen turvallisuusluokiteltujen tietojen vaihtamista Suomen hallituksen ja Naton välillä vastuullisten turvallisuusviranomaisten on vastavuoroisesti todettava hyväksymällään tavalla, että tiedot vastaanottava osapuoli on valmis suojaamaan saamansa tiedot luovuttajan edellyttämällä tavalla.

Tämän vakuudeksi edellä mainitut edustajat ovat allekirjoittaneet tämän sopimuksen.

Tehty Brysselissä 22 päivänä syyskuuta 1994 kahtena englannin- ja ranskankielisenä kappaleena, joiden molemmat tekstit ovat yhtä todistusvoimaiset.

Suomen hallituksen puolesta

Olli Mennander

Pohjois-Atlantin liiton puolesta

Sergio Balanzino

Article 5

Prior the exchange of any classified information between the Government of Finland and NATO, the responsible security authorities must reciprocally establish to their satisfaction that the recipient party is prepared to protect the information it receives, as required by the originator.

In witness whereof the above-mentioned Representatives have signed the present Agreement.

Done in duplicate at Brussels, this 22nd day of September 1994, in the English and French languages, both texts being equally authoritative.

For the Government of Finland

Mr. *Olli Mennander*

For the North Atlantic Treaty Organization

Mr. *Sergio Balanzino*