24.3.2023

Hallituksen esitys eduskunnalle tietoturvallisuudesta Pohjois-Atlantin sopimuksen osapuolten välillä tehdyn sopimuksen ja turvallisuussääntöjen hyväksymiseksi ja voimaansaattamiseksi ja Suomen ja Pohjois-Atlantin liiton kesken vaihdettavan turvallisuusluokitellun tiedon suojaamiseksi tehdyn hallinnollisen järjestelyn ja Pohjois-Atlantin liiton kanssa tehdyn tietoturvallisuussopimuksen irtisanomiseksi

ESITYKSEN PÄÄASIALLINEN SISÄLTÖ

Esityksessä ehdotetaan, että eduskunta hyväksyisi tietoturvallisuudesta Pohjois-Atlantin sopimuksen osapuolten välillä tehdyn sopimuksen ja turvallisuussäännöt sekä lain, jolla saatetaan voimaan sopimuksen ja turvallisuussääntöjen lainsäädännön alaan kuuluvat määräykset. Esityksessä ehdotetaan myös, että eduskunta antaisi suostumuksensa siihen, että Suomi irtisanoo Suomen ja Pohjois-Atlantin liiton kesken vaihdettavan turvallisuusluokitellun tiedon suojaamiseksi tehdyn hallinnollisen järjestelyn ja Pohjois-Atlantin liiton kanssa tehdyn tietoturvallisuussopimuksen.

Pohjois-Atlantin sopimuksen osapuolten välillä tehty tietoturvallisuussopimus on osa Pohjois-Atlantin liiton (Nato) oikeudellisesti sitovaa sopimuskehikkoa, johon Pohjois-Atlantin sopimukseen liittyvien uusien jäsenmaiden edellytetään sitoutuvan. Sopimus sisältää Pohjois-Atlantin sopimuksen osapuolten välillä sovellettavat määräykset turvallisuusluokitellun tiedon vastavuoroisesta suojaamisesta ja turvaamisesta. Monenvälinen sopimus korvaa Suomen kahdenväliset tietoturvallisuusjärjestelyt Pohjois-Atlantin liiton kanssa.

Sopimus tietoturvallisuudesta Pohjois-Atlantin sopimuksen osapuolten välillä on tehty Brysselissä 6.3.1997 ja se on tullut kansainvälisesti voimaan 16.8.1998. Sopimus tulee Suomen osalta voimaan kolmenkymmenen päivän kuluttua siitä päivästä, kun Suomi tallettaa tietoturvallisuussopimusta koskevan liittymiskirjansa Amerikan yhdysvaltojen hallituksen huostaan. Sopimuksen ja turvallisuussääntöjen voimaansaattamislaki on tarkoitettu tulemaan voimaan valtioneuvoston asetuksella säädettävänä ajankohtana samaan aikaan, kun sopimus tulee Suomen osalta voimaan. Laki Suomen ja Pohjois-Atlantin liiton kesken vaihdettavan turvallisuusluokitellun tiedon suojaamiseksi tehdyn hallinnollisen järjestelyn ja Pohjois-Atlantin liiton kanssa tehdyn tietoturvallisuussopimuksen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta annetun lain kumoamisesta on tarkoitettu tulemaan voimaan valtioneuvoston asetuksella säädettävänä ajankohtana samanaikaisesti, kun kyseisten sopimusten irtisanominen tulee voimaan.

SISÄLLYS

PERUSTELUT

1 Asian tausta ja valmistelu

1.1 Sopimus Pohjois-Atlantin sopimuksen osapuolten välillä tietoturvallisuudesta

Pohjois-Atlantin sopimuksen osapuolten välillä vuonna 1997 tietoturvallisuudesta tehdyn sopimuksen (jäljempänä myös tietoturvallisuussopimus) mukaan tehokas poliittinen neuvottelu, yhteistyö ja suunnittelu puolustusasioissa sopimuksen tavoitteiden saavuttamiseksi edellyttävät turvallisuusluokitellun tiedon vaihtamista osapuolten välillä. Tiedon vaihtamiseksi tarvitaan määräyksiä sellaisen turvallisuusluokitellun tiedon vastavuoroisesta suojaamisesta ja turvaamisesta. Sopimuksen tarkoituksena on asettaa turvallisuusvaatimuksille ja menettelyille yleiset puitteet.

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.

Tietoturvallisuussopimuksessa määritellään Naton ja sen jäsenvaltioiden turvallisuusluokiteltu tieto, johon sopimusta sovelletaan. Sopimuksen keskeinen lähtökohta on, että osapuolet säilyttävät tiedon turvallisuusluokituksen ja pyrkivät kaikin keinoin turvaamaan tietoa. Tietoa ei luovuteta kolmansille osapuolille ilman tiedon luovuttajan suostumusta. Sopimuksen toimeenpanoa varten osapuolilla tulee olla kansallinen turvallisuusviranomainen. Sopimuksen mukaan luottamuksellista (CONFIDENTIAL) ja sitä ylempiin turvallisuusluokkiin kuuluvaa tietoa käsittelevillä henkilöillä tulee olla asianmukainen turvallisuusselvitys.

Sopimuksen mukaan osapuolet laativat turvallisuusvaatimuksia, joilla varmistetaan turvallisuusluokitellun tiedon yhteinen suojauksen taso. Naton turvallisuussääntöjen vaatimukset koskevat henkilöstöturvallisuutta, tietoaineistoturvallisuutta, toimitilaturvallisuutta, viestintä- ja tietojärjestelmien turvallisuutta sekä yritysturvallisuutta.

Vuonna 1997 tehdyllä sopimuksella on korvattu osapuolten välillä vuonna 1952 tehty turvallisuussopimus. Pohjois-Atlantin liiton kaikki nykyiset jäsenvaltiot ovat tietoturvallisuussopimuksen osapuolia.

1.2 Suomen ja Pohjois-Atlantin liiton kesken vaihdettavan turvallisuusluokitellun tiedon suojaamiseksi tehty hallinnollinen järjestely ja Pohjois-Atlantin liiton kanssa tehty tietoturvallisuussopimus

Suomen ja Pohjois-Atlantin liiton välinen tietoturvallisuussopimus (*Security Agreement between Finland and the North Atlantic Treaty Organization*) allekirjoitettiin 22.9.1994 Suomen liityttyä Naton rauhankumppanuusohjelmaan (*Partnership for Peace, PfP*). Sopimuksessa sovittiin turvallisuusluokitellun aineiston vaihtamisesta ja suojaamisesta.

Suomen ja Naton välisellä 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 Suomi sitoutui olemaan käyttämättä Naton tiloja epäasialliseen toimintaan. Lisäksi ulkoasiainministeriön 13.9.1994 tekemällä päätöksellä hyväksyttiin tietoturvallisuussopimukseen liittyvät kaksi hallinnollisluonteista asiakirjaa (turvallisuusluokiteltua tietoa koskevat minimistandardit ja toimeenpanojärjestely) ja nimettiin sopimuksessa edellytetyksi informaatio- ja asiakirjaturvallisuuskysymyksistä vastaavaksi hallintoviranomaiseksi ulkoasiainministeriö. Päätöksen esittelymuistiossa hallintoviranomaisen tehtävät yksilöidään viittaamalla kansallisen sopimuksessa tarkoitetun turvallisuusviranomaisen tehtäviin sekä keskusrekisteriin (*Central Registry).*

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 ja 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.

Vuonna 2012 valtioneuvoston yleisistunto asetti valtuuskunnan neuvottelemaan vuoden 1994 tietoturvallisuussopimusta täydentävän hallinnollisen järjestelyn, jonka tarkoituksena oli ajantasaistaa vuoden 1994 sopimus siten, että siinä otetaan huomioon kansainvälisistä tietoturvallisuusvelvoitteista annetun lain säännökset sekä ajantasaistetut turvallisuusmääräykset. Tämän mukaisesti osapuolet neuvottelivat keväällä 2012 sopimusta täydentävän järjestelyn, joka allekirjoitettiin Helsingissä 3.7.2012. Hallinnollinen järjestely sisältää muun muassa määräykset turvallisuusluokitellun tiedon merkitsemisestä, tiedon suojaamisesta ja pääsystä tietoon, turvallisuusvaatimusten yksityiskohdista ja turvallisuustarkastuksista. Hallinnollisen järjestelyn kansallisen hyväksymisen yhteydessä saatettiin kansallisesti voimaan myös vuonna 1994 tehty Suomen ja Naton välinen tietoturvallisuussopimus (SopS 7 ja 8/2013). Hallinnollisen järjestelyn sekä vuonna 1994 tehdyn tietoturvallisuussopimuksen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta 21.12.2012 annettu laki (945/2012) tuli voimaan 1.2.2013. Suomen liittyessä Naton monenväliseen tietoturvallisuussopimukseen nämä kahdenväliset tietoturvallisuusjärjestelyt on tarkoitus irtisanoa sekä niiden voimaansaattamislaki kumota.

1.3 Valmistelu

Sopimuksen valmistelu

Tasavallan presidentti päätti 17.5.2022 valtioneuvoston esityksestä, että Suomi ilmoittaa Pohjois-Atlantin liitolle kiinnostuksesta käydä keskustelut Natoon liittymisestä ja nimitti Suomen

valtuuskunnan liittymiskeskusteluihin. Suomen kiinnostuksenosoitus esitettiin Naton pääsihteerille ulkoministerin kirjoittamalla kirjeellä, joka luovutettiin Brysselissä 18.5.2022. Naton jäsenvaltioiden päämiehet kutsuivat Suomen liittymiskeskusteluihin 29.6.2022 Madridin huippukokouksen yhteydessä.

Suomen ja Naton väliset liittymiskeskustelut käytiin Naton päämajassa Brysselissä 4.7.2022. Liittymiskeskusteluissa katettiin viisi osa-aluetta: 1) poliittiset kysymykset ja terrorismin torjunnan politiikkaan liittyvät kysymykset, 2) puolustus- ja sotilaalliset kysymykset, 3) resurssikysymykset, 4) tietoturvallisuuteen liittyvät kysymykset ja 5) oikeudelliset kysymykset. Liittymiskeskustelujen mukaan Suomen tulee liittyä seuraaviin kuuteen Naton sopimukseen 12 kuukauden sisällä Pohjois-Atlantin sopimusta koskevan Suomen liittymiskirjan tallettamisesta: sopimus Pohjois-Atlantin sopimuksen sopimuspuolten välillä niiden joukkojen asemasta (Nato SOFA), pöytäkirja Pohjois-Atlantin sopimuksen mukaisesta perustettujen kansainvälisten sotilasesikuntien asemasta (Pariisin pöytäkirja), sopimus teknisten tietojen välittämisestä puolustustarkoituksiin, sopimus puolustukseen liittyvien, patentoitavaksi haettujen keksintöjen salassapidon vastavuoroiseksi turvaamiseksi, sopimus Pohjois-Atlantin sopimuksen osapuolten välillä tietoturvallisuudesta sekä Pohjois-Atlantin osapuolten välinen sopimus ydinpuolustustietoja koskevasta yhteistyöstä.

Liittymiskeskustelujen jälkeen tasavallan presidentti päätti 4.7.2022 valtioneuvoston ratkaisuehdotuksesta, että Suomi toimittaa Pohjois-Atlantin liitolle aiekirjeen liittymisestä Pohjois-Atlantin sopimukseen. Aiekirje toimitettiin Natolle 5.7.2022, ja Pohjois-Atlantin sopimuksen osapuolet allekirjoittivat Suomen liittymispöytäkirjan samana päivänä.

Kansallinen valmistelu

Valtioneuvoston yleisistunto asetti 15.9.2022 koordinaatioryhmän ja sen alatyöryhmät valmistelemaan hallituksen esitystä Pohjois-Atlantin sopimuksen hyväksymisestä. Hallituksen esitys eduskunnalle Pohjois-Atlantin sopimuksen sekä Pohjois-Atlantin liiton, kansallisten edustajien ja kansainvälisen henkilöstön asemasta tehdyn sopimuksen hyväksymiseksi ja voimaansaattamiseksi (HE 315/2022 vp) annettiin 5.12.2022.

Edellä mainitut kuusi sopimusta päätettiin valmistella ja esittää hyväksyttäviksi erillisinä hallituksen esityksinä. Ulkoministeriö asetti 5.12.2022 työryhmän valmistelemaan hallituksen esitystä Naton tietoturvallisuussopimuksen hyväksymisestä. Työryhmässä olivat edustettuina ulkoministeriö, puolustusministeriö, oikeusministeriö, Suojelupoliisi ja Liikenne- ja viestintävirasto Traficom. Työryhmä kokoontui yhteensä 11 kertaa. Työryhmä kuuli valmistelun aikana tasavallan presidentin kansliaa ja ministeriöitä, joilla ei ollut edustajaa työryhmässä. Valtioneuvoston kanslia, valtiovarainministeriö, työ- ja elinkeinoministeriö, sosiaali- ja terveysministeriö sekä maa- ja metsätalousministeriö osallistuivat kuulemiseen.

Työryhmä sai hallituksen esityksen muotoon laaditun mietintönsä valmiiksi 22.3.2023.

Hallituksen esitysluonnoksesta pyydettiin lausuntoa muun muassa ministeriöiltä ja muilta viranomaisilta, elinkeinoelämän edustajilta sekä järjestöiltä yhteensä xx taholta ajalla 24.3.–21.4.2023 Lausuntopalvelu.fi –palvelun kautta. Annetut lausunnot sekä lausuntoyhteenveto ovat saatavilla valtioneuvoston hankesivuilla hankenumerolla UM001:00/2023.

2 Voimassa oleva lainsäädäntö ja sen arviointi

2.1 Laki kansainvälisistä tietoturvallisuusvelvoitteista

Lain yleinen soveltamisala

Lakia kansainvälisistä tietoturvallisuusvelvoitteista (588/2004) sovelletaan erityissuojattaviin tietoaineistoihin. Näillä tarkoitetaan sellaisia salassa pidettäviä asiakirjoja ja materiaaleja sekä asiakirjoista ja materiaaleista saatavissa olevia tietoja sekä näiden perusteella tuotettuja asiakirjoja ja materiaaleja, jotka kansainvälisen tietoturvallisuusvelvoitteen mukaisesti on turvallisuusluokiteltu. Määräysvalta erityissuojattavaan tietoaineistoon säilyy luovutuksen jälkeenkin aineiston luovuttaneella valtiolla, kansainvälisellä järjestöllä tai toimielimellä. Lakia voidaan soveltaa vain, jos kansainvälinen sopimus on saatettu Suomessa voimaan perustuslaissa säädetyllä tavalla tai jos kysymys on Suomea muutoin sitovasta kansainvälisestä tietoturvallisuusvelvoitteesta.

Lain soveltamisalan piiriin kuuluvia erityissuojattavia tietoaineistoja ovat lisäksi Suomen viranomaisen tai lain soveltamisalan piiriin kuuluvan elinkeinonharjoittajan laatimat asiakirjat, joista ilmenee Suomeen toimitettuihin erityissuojattaviin tietoaineistoihin sisältyviä tai tällaisista saatavissa olevia tietoja. Lakia ei sovelleta pelkästään Suomen kansallista tietoa sisältävien asiakirjojen tai niiden osien salassapitoon tai luokitukseen.

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

Todistuksen antamista koskevaan arvioon sekä todistuksen voimassaoloon ja peruuttamiseen sovelletaan turvallisuusselvityslakia (726/2014) (kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 11 §:n 2 momentti ja 12 §:n 2 momentti). Jos kansallinen turvallisuusviranomainen kieltäytyy antamasta henkilö- tai yritysturvallisuusselvitystodistusta, sen tulee ilmoittaa syyt tähän selvityksen hakijalle ja sen kohteelle annettavassa kirjallisessa päätöksessä (kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 11 §:n 3 momentti ja 12 §:n 3 momentti). Muutoksenhausta säädetään lain 20 a §:ssä.

Kansainvälisistä tietoturvallisuusvelvoitteista annettua lakia on tarkistettu sen säätämisen jälkeen tähän mennessä kuusi kertaa. Laki tarjoaa asianmukaisen säädöskehikon edelleen myös Naton tietoturvallisuussopimuksen täytäntöönpanolle Suomessa. Tietoturvallisuussopimus ei edellytä lain muuttamista, mutta lain 20-vuotisen soveltamiskäytännön valossa on jatkossa hyödyllistä arvioida mahdollisia tarkistustarpeita.

Lain suhde julkisuus- ja tiedonhallintalainsäädäntöön

Perustuslain (731/1999) sananvapautta ja julkisuutta koskevan 12 §:n mukaan viranomaisen hallussa olevat asiakirjat ja muut tallenteet ovat julkisia, jollei niiden julkisuutta ole välttämättömien syiden vuoksi erikseen rajoitettu, ja jokaisella on oikeus saada tieto julkisesta asiakirjasta ja tallenteesta. Julkisuusperiaatetta vahvistettiin Suomen valtiosäännössä perusoikeusuudistuksen yhteydessä, kun silloiseen hallitusmuotoon otettiin säännös oikeudesta saada tieto viranomaisen hallussa olevasta asiakirjasta ja muusta tallenteesta (HE 309/1993 vp, s. 58 ja PeVM 25/1994 vp, s. 9). Perustuslain 12 §:n 2 momentista johdettavaa julkisuusperiaatetta ilmentää

viranomaisten toiminnan julkisuudesta annetun lain (621/1999, jäljempänä julkisuuslaki) 1 §. Julkisuuslain 1 §:n 1 momentin mukaan viranomaisten asiakirjat ovat julkisia, jollei julkisuuslaissa tai muussa laissa erikseen toisin säädetä. Julkisuuslain esitöiden mukaan säännös vahvistaa julkisuusperiaatetta keskeisenä julkishallinnon periaatteena Suomessa. Pykälän tarkoitus on myös painottaa, että julkisuusperiaate on pääsääntö, josta voidaan poiketa vain lailla.

Naton asiakirjoihin ei lähtökohtaisesti järjestön omien säännösten tai käytäntöjen perusteella sovelleta julkisuusperiaatetta, eikä järjestön osalta ole säädetty yleisestä lähtökohtaisesta tiedonsaantioikeudesta sen asiakirjoihin.

Suomen viranomaisten hallussa oleviin asiakirjoihin sovelletaan julkisuuslakia, jollei laissa toisin säädetä. Julkisuuslain mukaan viranomaisen asiakirjoja ovat viranomaisen toimialalla tehtäviä hoidettaessa laaditut ja viranomaiselle toimitetut asiakirjat, jotka ovat viranomaisen hallussa (5 §). Toisin sanoen sekä viranomaisen itsensä laatimat Nato-yhteistyötä koskevat asiakirjat että viranomaisen hallussa olevat muut asiakirjat, jotka on saatu Nato-yhteistyön puitteissa, ovat julkisuuslaissa tarkoitettuja viranomaisen asiakirjoja. Naton turvallisuusluokiteltuihin asiakirjoihin sovelletaan kansainvälisistä tietoturvallisuusvelvoitteista annetun lain erityissäännöstä ehdottomasta salassapidosta, eikä näihin asiakirjoihin kohdistu julkisuuslain mukaista salassapidon vahinkoedellytyslausekkeiden arviointia. Naton turvallisuusluokitellut asiakirjat on siten pidettävä salassa, jollei niitä koskevista sopimuksista tai säännöistä muuta johdu.

Viranomaisen laatimat asiakirjat tulevat julkisuuslain mukaisen tiedonsaantioikeuden piiriin, kun asian käsittelyssä on saavutettu julkisuuslain 6 §:ssä säädetty ajankohta. Vastaavasti viranomaiselle toimitettujen asiakirjojen julkisuus alkaa siitä hetkestä, kun ne ovat saapuneet viranomaiselle (7 §). Mainittujen ajankohtien jälkeen tieto on annettava asiakirjasta, jollei salassapitosäännöksistä tai muista tiedon saantia rajoittavista säännöksistä muuta johdu. Tiedon antaminen sisällöltään julkisesta asiakirjasta ennen julkiseksi tulemisen ajankohtaa on viranomaisen harkinnassa (9 §).

Naton turvallisuussäännöstön mukaan Naton julkista tietoa on sellainen Naton tieto, jota ei ole turvallisuusluokiteltu ja jonka asiasta vastuussa oleva Naton toimielin tai virasto saattaa julkiseksi. Naton sisäiseen käyttöön tarkoitettu tieto, jota ei ole turvallisuusluokiteltu, merkitään NATO UNCLASSIFIED (NU). Tällaista tietoa saa luovuttaa turvallisuussäännöstön mukaan vain henkilöille, joilla on tarve tietoon (need-to-know). Asiakirjan ollessa Suomen viranomaisen hallussa, arvioidaan sen julkisuutta julkisuuslain perusteella.

Julkisuuslain lähtökohtana on, että asiakirjan salassapito perustuu laissa säädettyihin salassapitoperusteisiin, ja tieto julkisesta asiakirjasta voidaan luovuttaa ilman, että arvioidaan tiedon pyytäjän tarvetta pyydettyyn tietoon. Tietojensaantioikeutta voidaan perustuslain mukaan rajoittaa vain laissa määriteltyjen, välttämättömäksi katsottujen etujen turvaamiseksi. Julkisuuslain 24 §:ään sisältyvät yleiset säännökset asiakirjojen salassapitovelvoitteista. Nato-yhteistyöhön liittyvien asiakirjojen julkisuuden määräytymisen kannalta keskeisin salassapitosäännös on lain 24 §:n 1 momentin 2 kohta. Lainkohdassa tarkoitetut asiakirjat ovat salassa pidettäviä, jos tiedon antaminen niistä aiheuttaisi vahinkoa tai haittaa Suomen kansainvälisille suhteille tai edellytyksille toimia kansainvälisessä yhteistyössä. Lainkohdan perusteella salassa pidettäviä voivat olla esimerkiksi kansainvälisen yhteisön tai toimielimen laatimat asiakirjat, jos ne yhteisössä tai toimielimessä ovat salassa pidettäviä (HE 30/1998 vp). Muita kyseeseen tulevia salassapitosäännöksiä voivat olla julkisuuslain 24 §:n 1 momentin 1 ja 7-10 kohdat.

Kansainvälisistä tietoturvallisuusvelvoitteista annettuun lakiin sisältyy kansallisten asiakirjojen tietoturvallisuudesta annetuista säännöksistä poikkeavia säännöksiä. Lain 3 §:n 1 momentissa on kuitenkin yleinen viittaussäännös julkisuuslakiin sekä julkisen hallinnon tiedonhallinnasta

annettuun lakiin (906/2019, jäljempänä tiedonhallintalaki). Niiltä osin kuin suomalaisten viranomaisten asiakirjoihin sisältyy kansainvälisten tietoturvallisuusvelvoitteiden piiriin kuuluvia tietoja kansainvälisestä yhteistyöstä, on näihin tietoihin sovellettava kansainvälisistä tietoturvallisuusvelvoitteista annetun lain säännöksiä. Muilta osin sovelletaan julkisuus- ja tiedonhallintalakia ja niiden nojalla annettuja säännöksiä. Kuten edellä on todettu, julkisuuslaissa säädetään muun muassa oikeudesta saada tieto viranomaisten julkisista asiakirjoista sekä viranomaisessa toimivan vaitiolovelvollisuudesta ja asiakirjojen salassapidosta. Tiedonhallintalaissa puolestaan säädetään viranomaisten tietoaineistojen tiedonhallinnasta ja tietojärjestelmien käytöstä. Tiedonhallintalain 4 luvussa säädetään yleisistä tietoturvallisuustoimenpiteistä, jotka liittyvät kansainvälisiä tietoturvallisuusvelvoitteita mukaillen erityistä luotettavuutta edellyttävien tehtävien tunnistamiseen ja luotettavuudesta varmistumiseen (12 §), tietoaineistojen ja tietojärjestelmien tietoturvallisuuteen (13 §), tietojen siirtämiseen tietoverkossa (14 §), tietoaineistojen turvallisuuden varmistamiseen (15 §), tietojärjestelmien käyttöoikeuksien hallintaan (16 §), lokitietojen keräämiseen (17 §) ja asiakirjojen turvallisuusluokitteluun valtionhallinnossa (18 §).

Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 3 §:n 2 momentin mukaan julkisuuslakiin tai muuhun lakiin perustuvan pyynnön saada tieto erityissuojattavasta tietoaineistosta käsittelee ja ratkaisee se viranomainen, jolle tietoaineisto on toimitettu taikka jonka käsiteltäväksi asia kokonaisuudessaan kuuluu. Mainitun lain 6 §:n 1 momentissa säädetään erityisestä salassapitoperusteesta, jonka mukaan erityissuojattava tietoaineisto on pidettävä salassa, jollei kansainvälisestä tietoturvallisuusvelvoitteesta muuta johdu. Lain 7 §:n 2 momentin mukaan viranomaiseen palvelussuhteessa olevan ja viranomaisessa muutoin toimivan samoin kuin viranomaisen toimeksiannosta toimivan ja tämän palveluksessa olevan vaitiolovelvollisuudesta sekä siihen liittyvästä hyväksikäyttökiellosta on voimassa, mitä viranomaisten toiminnan julkisuudesta annetussa laissa säädetään. Lain 8 §:n 1 momentin mukaan erityissuojattavaan tietoaineistoon on siitä riippumatta, mitä julkisen hallinnon tiedonhallinnasta annetussa laissa tai sen nojalla säädetään, tehtävä kansainvälisessä tietoturvallisuusvelvoitteessa määritelty luokittelumerkintä sen osoittamiseksi, minkälaisia tietoturvallisuusvaatimuksia sen käsittelyssä on noudatettava.

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

Lisäksi julkisuuslain 30 §:ssä säädetään, että sen lisäksi, mitä laissa erikseen säädetään, viranomainen voi antaa salassa pidettävästä asiakirjasta tiedon ulkomaan viranomaiselle tai kansainväliselle toimielimelle, jos ulkomaan ja Suomen viranomaisen välisestä yhteistyöstä määrätään Suomea sitovassa kansainvälisessä sopimuksessa tai säädetään Suomea velvoittavassa säädöksessä ja tieto asiakirjasta voitaisiin tämän lain mukaan antaa yhteistyötä Suomessa hoitavalle viranomaiselle. Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 17 §:n mukaan Suomen viranomaisilla on vastaavalla tavalla oikeus antaa toiselle sopimuspuolelle kansainvälisen tietoturvallisuusvelvoitteen toteuttamiseksi välttämättömiä asiakirjoja ja tietoja sen estämättä, mitä asiakirjojen ja tietojen salassapidosta Suomen lainsäädännössä säädetään.

Lain soveltaminen elinkeinonharjoittajiin

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

Turvallisuusluokitellulla sopimuksella tarkoitetaan sopimusta, jonka toisen valtion viranomainen tai siellä kotipaikkaansa pitävä yritys taikka kansainvälinen järjestö tai toimielin aikoo tehdä tai on tehnyt kansainvälisessä tietoturvallisuusvelvoitteessa tarkoitetulla tavalla Suomessa kotipaikkaansa pitävän elinkeinonharjoittajan kanssa, jos tarjouskilpailuun osallistuminen tai sopimuksen toteuttaminen voi edellyttää pääsyä erityissuojattavaan tietoaineistoon (2 §:n 1 momentin 3 kohta).

Elinkeinonharjoittajalla ja tämän palveluksessa tai toimeksiannosta toimivalla on erityissuojattavia tietoaineistoja koskeva salassapitovelvollisuus, velvollisuus käyttää tällaista tietoaineistoa vain siihen tarkoitukseen, jota varten se on annettu sekä velvollisuus pitää huolta siitä, että tietoaineistoon on pääsy vain niillä, jotka tarvitsevat tietoa tehtävän hoitamisessa (6 §). Elinkeinonharjoittajalla on myös velvollisuus antaa toimivaltaiselle turvallisuusviranomaiselle tietoja kansainvälisten tietoturvallisuusvelvoitteiden toteuttamiseksi sekä sallia viranomaisen ja kansainvälisen toimielimen tai sopimusvaltion edustajan tutustuminen turvallisuusjärjestelyihinsä ja toimitiloihinsa (16 §:n 2 momentti ja 18 §:n 2 momentti).

Lain täytäntöönpanoviranomaiset

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

Tietojen salassapito ja käytön sääntely

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

Turvallisuusluokittelu ja suojaamistoimenpiteet

Kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa säädetään velvollisuudesta merkitä erityissuojattavaan tietoaineistoon sen turvallisuusluokka. Erityissuojattavaan tietoaineistoon on tehtävä luokittelumerkintä, joka osoittaa, minkälaisia tietoturvallisuusvaatimuksia sen käsittelyssä on noudatettava (8 §). Mitä korkeampaan turvallisuusluokkaan aineisto kuuluu, sitä

tiukempia tietoturvallisuustoimenpiteitä edellytetään. Laissa on yleinen velvoite toteuttaa tietoaineiston käsittelyssä sen turvallisuusluokkaa koskevia käsittelymääräyksiä sekä valtuus säätää erityissuojattavan tietoaineiston käsittelyssä noudatettavista eri turvallisuusluokkia vastaavista turvallisuustoimenpiteistä valtioneuvoston asetuksella (9 §). Asiakirjojen turvallisuusluokittelusta valtionhallinnossa annetun valtioneuvoston asetuksen (1101/2019, jäljempänä turvallisuusluokitteluasetus) 4 §:ssä säädetään turvallisuusluokituksen vastaavuudesta kansainvälisiä tietoturvallisuusvelvoitteita toteutettaessa. Säännöstä sovelletaan, jollei kansainvälisestä tietoturvallisuusvelvoitteesta muuta johdu.

Erityissuojattava tietoaineisto on kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 10 §:n mukaan säilytettävä tiloissa, joissa asiakirjojen ja materiaalien sekä niihin sisältyvien tietojen suojaamisesta voidaan huolehtia kansainvälisessä tietoturvallisuusvelvoitteessa edellytetyllä tavalla. Tilojen turvallisuusvaatimuksista säädetään turvallisuusluokitteluasetuksen 9 ja 10 §:ssä.

Lakiin kansainvälisistä tietoturvallisuusvelvoitteista on kirjattu kansainvälisissä sopimuksissa oleva yleinen vaatimus siitä, että erityissuojattavaan tietoaineistoon annetaan pääsy vain niille, jotka tarvitsevat tietoja tehtäviensä hoitamisessa. Nämä henkilöt on nimettävä etukäteen, jos kansainvälisessä tietoturvallisuusvelvoitteessa tätä edellytetään (lain 6 §:n 3 momentti). Sama koskee myös 1 §:n 2 momentissa tarkoitettua elinkeinonharjoittajaa.

Tietojärjestelmäturvallisuus

Liikenne- ja viestintävirasto toimii kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 4 §:n mukaan kansallisen turvallisuusviranomaisen asiantuntijana tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuutta koskevissa asioissa ja vastaa muun muassa kansainvälisten tietoturvallisuusvelvoitteiden edellyttämistä tietojärjestelmien arvioinnista ja hyväksyntätehtävistä (akkreditointi). Viranomaisten tietojärjestelmien tietoturvallisuuden arviointia koskevasta menettelystä ja Liikenne- ja viestintäviraston tietoturvallisuuden arviointitehtävästä säädetään viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista annetussa laissa (1406/2011, jäljempänä arviointilaki). Viranomaiset voivat käyttää tietojärjestelmäarvioinneissa myös laissa tietoturvallisuuden arviointilaitoksista (1405/2011) tarkoitettuja Liikenne- ja viestintäviraston hyväksymiä arviointilaitoksia. Toistaiseksi arviointilaitoksia ei ole hyväksytty tekemään EU:n tai Naton turvallisuusluokiteltuja tietoja käsittelevien tietojärjestelmien arviointeja. Yritysten tietojärjestelmien arvioinnista osana yritysturvallisuusselvitystä säädetään turvallisuusselvityslaissa.

2.2 Turvallisuusselvityslaki

Lain tarkoitus ja soveltamisala

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

Laissa säädetään henkilö- ja yritysturvallisuusselvityksen laadinnassa noudatettavasta menettelystä. Laki sisältää säännökset turvallisuusselvityksen laatimisen edellytyksistä sekä sitä laadittaessa käytettävistä tiedoista, selvityksen kohteen suostumuksesta ja tiedonsaantioikeuksista, selvityksen hakijan ja selvityksen kohteen tiedonantovelvollisuuksista sekä turvallisuusselvityksen ja sen perusteella annetun todistuksen voimassaolosta ja todistuksen peruuttamisesta

sekä henkilörekisterien yhdistämisestä selvityksen kohteen nuhteettomuuden ja luotettavuuden seuraamiseksi ja sen johdosta suoritettavista toimenpiteistä (2 §). Turvallisuusselvitys voidaan tehdä vain selvityksen kohteen etukäteen antaman kirjallisen suostumuksen perusteella (5 §).

Henkilöstöturvallisuus

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

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

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

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

Turvallisuusselvityslain 43 §:n 2 momentin mukaan kansallinen turvallisuusviranomainen antaa kansainvälisen tietoturvallisuusvelvoitteiden toteuttamiseksi tarpeellisen henkilöturvallisuusselvitystodistuksen siten kuin kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa säädetään.

Yritysturvallisuus

Yritysturvallisuusselvityksellä tarkoitetaan turvallisuusselvityslain 3 §:n 1 momentin 2 kohdan mukaisesti yrityksen ja sen vastuuhenkilöiden luotettavuuden, yrityksen tietoturvallisuuden tason sekä sitoumustenhoitokyvyn arvioimiseksi turvallisuusselvityslaissa säädetyllä tavalla laadittavaa selvitystä yrityksestä. Selvitys voidaan laatia, jos selvitystä edellytetään kansainvälisen järjestön tai toimielimen säännöissä tai toisen valtion laissa ja jos se on tarpeen sen vuoksi, että selvityksen kohde voi tulla valituksi kansainvälisen järjestön tai toimielimen järjestämään tai näiden muutoin organisoimaan hankkeeseen taikka toisessa valtiossa järjestettävään hankintakilpailuun tai aloittaa yritystoiminnan toisessa valtiossa (36 § 2 momentti). Yritysturvallisuusselvitys voidaan laatia selvityksen kohteen pyynnöstä 36 §:n 2 momentissa tarkoitetuissa tapauksissa.

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

Yritysturvallisuusselvitystä laadittaessa selvitetään hakemuksessa esitettyjen tietojen ja 37 §:ssä tarkoitettujen tietolähteiden sekä yrityksen toimitilojen ja tietojärjestelmien tarkastuksen avulla, miten yritys huolehtii tietojen suojaamisesta, asiattoman pääsyn estämisestä tiloihin ja henkilöstön koulutuksesta (38 §:n 1 momentti). Lain 38 §:n mukaan yritysturvallisuusselvitys voidaan tehdä myös osittaisena, jos se on tarpeen kansainvälisen tietoturvallisuusvelvoitteen toteuttamiseksi tai muutoin perusteltua.

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

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

2.3 Henkilötietojen käsittelyä koskeva lainsäädäntö

Käsitellessään hallituksen esitystä 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 (HE 139/2012 vp) eduskunnan puolustusvaliokunta kiinnitti huomiota julkisuuden ja salassapitokysymysten ohella esityksen henkilötietojen suojaa koskeviin vaatimuksiin. Valiokunta totesi tuolloin saamansa selvityksen perusteella, että Suomen ja Naton väliseen hallinnolliseen järjestelyyn sisältyvät määräykset loivat riittävästi edellytyksiä henkilötietojen suojaa koskevien vaatimusten huomioimiselle julkisuus- ja salassapitonäkökohtien ohella. Valiokunta korosti, että hallinnollisen järjestelyn artikloja tulkittaessa ja sovellettaessa tulee huomioida perustuslain 12 §:ssä turvattu julkisuus ja 10 §:ssä suojattu henkilötietojen suoja siltä osin kuin turvallisuusluokiteltuihin tietoihin sisältyy henkilötietoja (PuVM 5/2012 vp).

Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 17 §:n mukaan Suomen viranomaisilla on oikeus antaa toiselle sopimuspuolelle kansainvälisen tietoturvallisuusvelvoitteen toteuttamiseksi välttämättömiä asiakirjoja ja tietoja sen estämättä, mitä asiakirjojen ja tietojen salassapidosta Suomen lainsäädännössä säädetään. Sanottu ei koske yksityisyyden suojan vuoksi salassa pidettäviksi säädettyjä tietoja. Turvallisuusselvityslain 26 §:ssä säädetään mahdollisuudesta hankkia kansainvälisen sopimuksen nojalla tietoja ulkomaan viranomaisen ylläpitämistä rekistereistä, 57 §:ssä viranomaisten tiedonsaantioikeudesta ja 59 §:ssä tietojen salassapitovelvollisuudesta.

Kansallisen turvallisuuden ylläpitäminen jää nimenomaisten EU:n yleisen tietosuoja-asetuksen (EU) 2016/679 ja rikosasioiden tietosuojadirektiivin (EU) 2016/680 säännösten perusteella niiden soveltamisalan ulkopuolelle. Suomessa rikosasioiden tietosuojadirektiivi on pantu täytäntöön lailla henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä (1054/2018, jäljempänä rikosasioiden tietosuojalaki). Rikosasioiden tietosuojadirektiivin soveltamisalarajoituksesta huolimatta rikosasioiden tietosuojalain soveltamisalaa on direktiivin liikkumavaran puitteissa ulotettu koskemaan henkilötietojen käsittelyä kansallisen turvallisuuden ja puolustuksen yhteydessä. Näin ollen Naton asiakirjojen sisältämien henkilö-

tietojen käsittelyyn sovelletaan lähtökohtaisesti rikosasioiden tietosuojalakia silloin kun käsittely kuuluu lain 1 §:n 2 momentin soveltamisalaan. Rikosasioiden tietosuojalain 1 §:n 2 momentin mukaan sen lisäksi, mitä 1 momentissa säädetään, lakia sovelletaan

1) Puolustusvoimien suorittamaan ja Puolustusvoimien lukuun suoritettavaan henkilötietojen käsittelyyn, kun tietoja käsitellään puolustusvoimista annetun lain (551/2007) 2 §:n 1 momentin 1 kohdassa, 2 kohdan a alakohdassa tai 3 ja 4 kohdassa säädettyjen tehtävien hoitamiseksi, sekä Puolustusvoimien pääesikunnan suorittamaan henkilötietojen käsittelyyn turvallisuusselvityslain 9 §:n 3 momentissa tarkoitettujen tehtävien hoitamiseksi;

2) poliisin suorittamaan henkilötietojen käsittelyyn, kun tietoja käsitellään sellaisessa poliisilain (872/2011) 1 luvun 1 §:n 1 momentissa tarkoitetussa tehtävässä, joka liittyy kansallisen turvallisuuden suojaamiseen, sekä turvallisuusselvityslain 9 §:n 1 momentissa tarkoitetuissa tehtävissä;

3) Rajavartiolaitoksen suorittamaan henkilötietojen käsittelyyn, kun tietoja käsitellään sellaisessa rajavartiolain (578/2005) 3 §:n 2 ja 3 momentissa tarkoitetussa tehtävässä, joka liittyy kansallisen turvallisuuden suojaamiseen.

Rikosasioiden tietosuojalain 7 luvussa säädetään toimivaltaisen viranomaisen suorittamasta henkilötietojen siirrosta kolmansiin maihin ja kansainvälisille järjestöille. Henkilötietojen käsittelystä Puolustusvoimissa annetun lain (332/2019) 2 §:n 1 momentissa on rajattu Puolustusvoimien suorittama tiedonvaihto rikosasioiden tietosuojalain 7 luvun soveltamisen ulkopuolelle. Puolustusvoimien suorittamasta henkilötietojen luovuttamisesta ulkomaille ja kansainvälisille järjestöille säädetään henkilötietojen käsittelystä Puolustusvoimissa annetun lain 4 luvussa.

Lisäksi Naton asiakirjojen sisältämien henkilötietojen käsittelyyn voidaan soveltaa rikosasioiden tietosuojalakia täydentäviä säädöksiä, kuten henkilötietojen käsittelystä poliisitoimessa annettua lakia (616/2019) ja henkilötietojen käsittelystä Puolustusvoimissa annettua lakia.

Naton asiakirjoihin sisältyviä henkilötietoja voivat käsitellä myös muut kuin rikosasioiden tietosuojalaissa tarkoitetut toimivaltaiset viranomaiset. Näiden viranomaisten suorittamaan henkilötietojen käsittelyyn sovelletaan tietosuojalain (1050/2018) 2 §:n 1 momentin mukaisesti EU:n yleistä tietosuoja-asetusta ja kansallista tietosuojalakia.

2.4 Eduskunnan tiedonsaantioikeus

Eduskunnan tietojensaanti- ja osallistumisoikeus Nato-asioissa turvataan perustuslain ja muun lainsäädännön nojalla. Valtiosäännön perusta on perustuslaissa säädetty kansanvallan periaate (2 § 1 momentti), jonka mukaan eduskunta on ylin valtioelin myös kansainvälisissä asioissa. Eduskunnan asema ylimpänä valtioelimenä saa tässä suhteessa konkreettista sisältöä menettelystä presidentin ja valtioneuvoston välisen näkemyseron ratkaisemisessa (58 § 2 momentti). Eduskunnan vaikutusmahdollisuudet tulee turvata myös ennakoivalla tavalla.

Valtioneuvosto on kokonaisvastuussa eduskunnan tiedonsaannista sekä osallistumismahdollisuuksien turvaamisesta. Parlamentaarisen hallitustavan periaatteen ja perustuslain 58 §:n ja 93 §:n säännösten perusteella valtioneuvosto on myös kokonaisvastuussa asioiden valmistelusta.

Eduskunnalla on perustuslain 47 §:n mukaan oikeus saada valtioneuvostolta asioiden käsittelyssä tarvitsemansa tiedot. Säännös sisältää yhtäältä valtioneuvoston velvollisuuden oma-aloitteisesti toimittaa eduskunnan tarvitsemat tiedot ja toisaalta velvollisuuden toimittaa eduskunnan

pyytämät tiedot (HE 1/1998 vp, s. 97). Asianomaisen ministerin tulee huolehtia siitä, että valiokunta tai muu eduskunnan toimielin saa viipymättä tarvitsemansa viranomaisen hallussa olevat asiakirjat ja muut tiedot. Ulkoasiainvaliokunnalle annetaan selvityksiä ulko- ja turvallisuuspolitiikkaa koskevista asioista perustuslain 97 §:n nojalla. Ulkoasiainvaliokunta voi saamiensa selvitysten perusteella tarvittaessa antaa oma-aloitteisen lausunnon valtioneuvostolle. Perustuslakivaliokunnan mukaan selvityksenantovelvollisuus myös presidentin ulkopoliittisesta toiminnasta on eduskunnan luottamuksen varassa toimivalla valtioneuvostolla (PeVM 9/2010 vp). Eduskunta on korostanut, että valtioneuvoston tulee oma-aloitteisesti pitää ulkoasiainvaliokunta informoituna oikea-aikaisesti ja säännönmukaisesti kansainvälisistä asioista. Eduskunnan rooli mahdollisena ristiriidan ratkaisijana edellyttää laaja-alaista tiedottamista myös asioiden valmistelu- ja keskusteluvaiheesta (PeVM 9/2010 vp ja UaVL 5/2010 vp).

Perustuslakivaliokunnan tulkinnan mukaan valiokunnan tietojensaantioikeuteen ei vaikuta se, että valiokunnan tarvitsemat tiedot olisivat esimerkiksi oikeudelliselta luonteeltaan salassa pidettäviä (PeVL 30/2020 vp s. 3). Myös eduskunnan ulkoasiainvaliokunta on korostanut, että eduskunnan tiedonsaantioikeus ulottuu myös salassa pidettäviin asiakirjoihin (UaVL 4/2020 vp s. 2). Eduskunnan tarkastusvaliokunta on todennut, että perusteet, joilla ministeriö voisi olla antamatta joitain tietoja eduskunnalle, voivat olla hyvin vähälukuisia ja etupäässä liittyä sellaisiin seikkoihin kuin tiedon ilmeisen selvä epäolennaisuus ja epäluotettavuus, spekulatiivisuus ja vanhentuneisuus. Joissain tilanteissa kansainväliseen yhteistyöhön liittyviin asiakirjoihin voi sisältyä sellaisia tietoja, joiden paljastuminen voi aiheuttaa merkittävää ja laajalle ulottuvaa vahinkoa keskeisille yleisille eduille, kuten Suomen suhteille ulkovaltoihin. Tällaisten aineistojen asianmukaisesta käsittelystä on pidettävä erityistä huolta, koska kysymys on Suomen luotettavuudesta kansainvälisen yhteistyön osapuolena. Tällaistenkin tietojen suhteen on ensisijainen menettelytapa perustuslain kannalta se, että valiokunnan jäseniltä edellytetään vaiteliaisuutta sen sijaan, ettei tietoa lainkaan anneta eduskunnalle. Perustuslaki ei tunne mahdollisuutta, että esim. turvallisuusluokiteltu tieto jätettäisiin antamatta eduskunnalle. (TrVM 2/2013 vp s. 3)

Sääntelyä valiokunnan jäsenten vaitiolovelvollisuudesta on perustuslain 50 §:n 2 ja 3 momentissa sekä eduskunnan työjärjestyksen 43 a–43 c §:ssä (PeVL 30/2020 vp, s. 3). Työjärjestyksen 43 c §:n 1 momentin mukaan valiokunnan jäsen tai virkamies ei saa paljastaa asiakirjan salassa pidettävää sisältöä tai tietoa, joka asiakirjaan merkittynä olisi salassa pidettävä, taikka sellaista seikkaa, josta valiokunta on tehnyt perustuslain 50 §:n 3 momentin mukaisen vaitiolopäätöksen. Vaiteliaisuus merkitsee siis myös sitä, että vaiteliaisuuden alaista asiaa käsittelevän valiokunnan jäsen ei voi vapaasti keskustella asiasta esimerkiksi ryhmäkokouksessa (PeVL 30/2020 vp, s. 18). Perustuslakivaliokunta on korostanut, että vaiteliaisuuden ala tulee rajata laajuudeltaan ja kestoltaan vain välttämättömään (PeVL 16/2020 vp s. 5-6). Valiokunnan jäsen tai virkamies ei saa myöskään käyttää salassa pidettäviä tietoja omaksi taikka toisen hyödyksi tai toisen vahingoksi. Rangaistus salassapitorikoksesta ja salassapitorikkomuksesta säädetään rikoslain 38 luvun 1 ja 2 §:ssä.

Naton turvallisuusluokitellun tiedon käsittelyä koskevat säännökset on otettava huomioon myös tietojen käsittelyssä eduskunnassa. Tämä tarkoittaa esimerkiksi Naton turvallisuussääntöjen mukaisia toimintamalleja (sisältäen tila-, henkilö- ja tiedonhallintaratkaisut sekä niihin liittyvät tekniset ratkaisut) ja henkilöturvallisuusselvitystodistusten myöntämistä soveltuvin osin. Valtioneuvoston oikeuskansleri on ottanut muistiossaan OKV/3212/24/2021 kantaa erityissuojattavia tietoaineistoja koskevaan eduskunnan tiedonsaantioikeuteen hävittäjien hankintaa koskevassa asiassa. Muistiossa todetaan, että kansainvälisissä tietoturvallisuusvelvoitteissa on usein keskeistä luovutettujen tietojen tiukka käyttötarkoitussidonnaisuus, jonka mukaan tiedot ovat käytettävissä vain tiettyyn nimenomaiseen tarkoitukseen. Tietojen käyttö muuhun tarkoitukseen edellyttää tiedot antaneen tahon suostumusta. Lisäksi sopimuksissa on sovittu erityissuojattavan

aineiston suojaamista koskevista erityisistä menettelyistä ja suojatoimista. Nykyisessä kansainvälisessä yhteistyössä tietoturvallisuutta koskevien velvoitteiden noudattamiseen kiinnitetään paljon huomiota ja tietoturvallisuusvelvoitteiden asianmukainen kunnioittaminen on keskeinen osa valtion mahdollisuuksia toimia kansainvälisessä yhteistyössä ja saada tietoja muilta valtioilta.

Eduskunnan asemasta ylimpänä valtioelimenä sekä lainsäädäntövaltaa ja valtiontaloudellista valtaa käyttävänä valtioelimenä seuraa, että eduskunnan on saatava luotettavat ja kattavat tiedot päätöksentekonsa perustaksi. Tämä on perustuslaissa säädettyjen kansanvaltaisen hallitusmuodon perusteiden toteuttamisen välttämätön edellytys. Parlamentaarisen järjestelmän toimintaan kuuluu välttämättömänä elementtinä tiedonkulku eduskunnan ja hallituksen välillä. Eduskunnan laaja tiedonsaantioikeus turvaa myös valtioneuvoston parlamentaarista valvontaa (PeVL 30/2020 vp s. 2-3.

3 Kansainvälinen kehitys sekä ulkomaiden ja EU:n lainsäädäntö

Turvallisuusluokiteltujen tietojen käsittelyä koskevissa kansainvälisissä sopimuksissa ja järjestelyissä on luotu pitkälti vakiintuneet menettelyt ja säännöt kansainvälisen luokitellun tiedon käsittelyssä. Suomella on tällä hetkellä tietoturvallisuussopimus 20 valtion kanssa sekä Pohjoismaiden, Euroopan unionin jäsenvaltioiden, Euroopan avaruusjärjestön, Euroopan puolustusmateriaalijärjestö OCCARin sekä Pohjois-Atlantin liiton kanssa. Suomi osallistuu myös Naton jäsenmaiden vuonna 1985 perustamaan monenväliseen epäviralliseen yritysturvallisuustyöryhmään (Multinational industrial security working group, *MISWG*), jossa valmistellaan yhteisiä menettelyitä ja sääntöjä turvallisuusluokiteltujen tietojen vaihdon käsittelyssä.

Euroopan unionissa on omaksuttu turvallisuusluokiteltujen tietojen käsittelystä Naton järjestelmää läheisesti muistuttavat menettelyt ja säännöt. Neuvoston osalta ne sisältyvät neuvoston päätökseen EU:n turvallisuusluokiteltujen tietojen suojaamista koskevista turvallisuussäännöistä (2013/488/EU). Päätöksen lisäys sisältää jäsenmaiden turvallisuusluokkien vastaavuudet. Neuvostossa kokoontuneet Euroopan unionin jäsenvaltiot tekivät vuonna 2015 sopimuksen Euroopan unionin edun vuoksi vaihdettujen turvallisuusluokiteltujen tietojen suojaamisesta (SopS 76 ja 77/2015). Komissio antoi 22.3.2022 ehdotuksen Euroopan parlamentin ja neuvoston asetukseksi tietoturvallisuudesta unionin toimielimissä, elimissä ja laitoksissa (COM(2022) 119 final), jonka käsittely neuvostossa ja Euroopan parlamentissa on kesken. Euroopan unioni on tehnyt vuonna 2003 Naton kanssa tietoturvallisuutta koskevan sopimuksen (2003/211/YUTP, EUVL L 80, 27.3.2003, s. 36).

Euroopan unionin jäsenvaltiot ovat osapuolina edellä mainitussa neuvostossa kokoontuneiden Euroopan unionin jäsenvaltioiden välisessä sopimuksessa Euroopan unionin edun vuoksi vaihdettujen turvallisuusluokiteltujen tietojen suojaamisesta. Kaikki nykyiset Naton jäsenvaltiot ovat osapuolina nyt hyväksyttävänä olevassa Naton tietoturvallisuussopimuksessa. Pohjoismaat ovat tehneet lisäksi sopimuksen Tanskan, Suomen, Islannin, Norjan ja Ruotsin välillä turvallisuusluokitellun tiedon vastavuoroisesta suojaamisesta ja vaihtamisesta (SopS 10-12/2013). Näin ollen Suomen viiteryhmän maiden kansainväliset velvoitteet ovat yhteneväiset. Kansallisten turvallisuusviranomaisten järjestäytyminen vaihtelee historiallisista syistä maittain. Esimerkiksi Ruotsissa kansallinen turvallisuusviranomainen (NSA) sijaitsee Suomen tavoin ulkoministeriössä, Tanskassa NSA sijaitsee tiedustelupalvelussa ja Norjassa kansallinen turvallisuusviranomainen (NSM) on poikkisektoraalinen ammatti- ja valvontaviranomainen, joka on järjestetty puolustusministeriön alaisuuteen, mutta raportoi siviilisektorin osalta oikeusministeriölle. Alankomaissa on kaksi kansallista turvallisuusviranomaista, AIVD ja MIVD. AIVD on osa sisäministeriötä. Sillä on yleisenä tiedustelu- ja turvallisuuspalveluna koordinoiva rooli, mutta molemmat on epävirallisesti nimetty kansalliseksi turvallisuusviranomaiseksi (NSA).

4 Sopimuksen tavoitteet

Pohjois-Atlantin sopimuksen osapuolten välillä tietoturvallisuudesta tehdyn sopimuksen johdannon mukaan tehokas poliittinen neuvottelu, yhteistyö ja suunnittelu puolustusasioissa sopimuksen tavoitteiden saavuttamiseksi edellyttävät turvallisuusluokitellun tiedon vaihtamista osapuolten välillä. Sen mahdollistaminen edellyttää määräyksiä turvallisuusluokitellun tiedon vastavuoroisesta suojaamisesta ja turvaamisesta. Sopimuksen tarkoituksena on luoda turvallisuusvaatimuksille ja menettelyille yleiset puitteet.

5 Keskeiset ehdotukset

Esityksessä ehdotetaan, että eduskunta hyväksyisi Pohjois-Atlantin sopimuksen osapuolten välillä tietoturvallisuudesta tehdyn sopimuksen ja turvallisuussäännöt. Esitys sisältää myös ehdotuksen niin sanotuksi blankettilaiksi, jolla saatetaan voimaan sopimuksen ja turvallisuussääntöjen lainsäädännön alaan kuuluvat määräykset. Lisäksi ehdotetaan, että eduskunta antaisi suostumuksensa siihen, että Suomi irtisanoo Suomen ja Pohjois-Atlantin liiton kesken vaihdettavan turvallisuusluokitellun tiedon suojaamiseksi tehdyn hallinnollisen järjestelyn ja Pohjois-Atlantin liiton kanssa tehdyn tietoturvallisuussopimuksen. Esitys sisältää ehdotuksen laiksi, jolla kumotaan kyseisten sopimusten lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta annettu laki (945/2012).

6 Esityksen vaikutukset

6.1 Taloudelliset vaikutukset

Natoon liittyminen aiheuttaa kertaluonteisia lisäkustannuksia ja pysyviä kiinteitä kustannuksia mm. tietoturvallisuusratkaisuihin ja toimitilaturvallisuuteen liittyen. Natoon liittyvän tiedon käsittelyn mahdollistavan ja korkeaa turvallisuutta edellyttävän tietojenkäsittely-ympäristön jatkokehittämiskustannusten arvioidaan tällä hetkellä olevan noin 20 miljoonaa euroa vuosina 2023-2025. Kulut koostuvat henkilöstö-, laite- ja ohjelmistomenoista. Korkeaa turvallisuutta edellyttävän tietojenkäsittelyratkaisun jatkokehittämiselle on varattu rahoitus vuosien 2022 ja 2023 talousarvioissa. Lisäksi tietojenkäsittelytiloihin vaadittavat suojaukset tulevat aiheuttamaan uusia kustannuksia arviolta noin kuusi miljoonaa euroa kohdistuen pääsääntöisesti vuokrauskustannuksiin. Tehtävät investoinnit tulevat aiheuttamaan noin kolmen miljoonan euron ylläpitokustannukset vuodesta 2026 lähtien.

Investointi- ja ylläpitorahoituksen lopullinen tarve tarkentuu suunnittelun ja toteutuksen edetessä. Välillisesti Nato-jäsenyydestä aiheutuvat tiloihin kohdistuvat kustannukset tarkentuvat vuoden 2023 aikana tehtävässä kartoituksessa. Muut mahdolliset lisäkustannukset, ml. tiedonvälitykseen ja toimitilaturvallisuuteen liittyen, selkiytyvät usean vuoden kuluessa. Nato-jäsenyyden myötä voi korkeaa turvallisuutta edellyttävän tiedonkäsittelyn määrän lisääntymisellä olla vaikutuksia Nato-tiedonkäsittelyn kustannuksiin. Pohjois-Atlantin sopimuksen osapuolten välillä tietoturvallisuudesta tehty sopimus ei kuitenkaan suoranaisesti lisää valtion yhteisen korkeaa turvallisuutta edellyttävän tietojenkäsittely ympäristön kustannuksia, koska vastaavat vaatimukset ovat olleet voimassa jo kumppanuusaikana.

Nato-jäsenyyden myötä lisääntyvästä Puolustusvoimien ja Naton välisestä suorasta tietojenkäsittelystä aiheutuvat lisäkustannukset sisältyvät Puolustusvoimien talousarvio- ja kehysesitykseen. Puolustusvoimien lisäkustannukset johtuvat välillisesti tietoturvallisuusvelvoitteiden toteuttamisesta, mutta suoranaisesti pääosin itse Nato-jäsenyydestä.

Jäsenyydestä aiheutuvat eri hallinnonalojen lisämäärärahatarpeet tullaan esittämään vuosittaisen julkisen talouden suunnitelman sekä talous- ja lisätalousarvioiden valmistelun yhteydessä niiden käyttötarkoituksen mukaisilta momenteilta.

6.2 Vaikutukset viranomaistoimintaan

Nato-jäsenyyden myötä keskeisimmät vaikutukset kansalliseen tietoturvallisuuteen syntyvät eri toimintojen järjestämisestä Naton tietoturvallisuusvaatimusten edellyttämälle tasolle. Suomi on tehnyt Naton kanssa turvallisuusluokitellun tiedon suojaamista koskevan sopimuksen ja sitä täydentävän hallinnollisen järjestelyn, minkä johdosta Suomi suojaa ja käsittelee Naton turvallisuusluokiteltua tietoa jo tällä hetkellä Naton turvallisuussääntöjen vähimmäisvaatimusten ja perusperiaatteiden mukaisesti. Vaatimukset koskevat henkilöstöturvallisuutta, tietoaineistoturvallisuutta, toimitilaturvallisuutta, viestintä- ja tietojärjestelmien turvallisuutta sekä yritysturvallisuutta. Naton tietoturvallisuussopimukseen sitoutuminen ei muuta nykytilannetta merkittävästi. Rauhankumppanuuden ja jäsenyyden aikana sovellettavien tietoturvallisuusvaatimusten vähäisiä eroja selostetaan jaksossa 8.2. Rauhankumppanuuden aikana vakiintuneet tietoturvallisuusprosessit muodostavat toimivan perustan myös niitä koskevalle kehitystyölle jäsenyyden alkaessa. Jäsenyyden myötä Naton turvallisuusluokiteltujen tietojen määrät kasvavat ja käsittelytarve laajenee eri viranomaisiin ja ministeriöihin sekä yrityksiin. Asiakirjojen määrän kasvua ja lisäystä eri hallinnonaloilla on kuitenkin vaikea arvioida ennen jäsenyyden alkua. Jäsenyyden myötä Suomi voi saada myös Naton korkeimman turvaluokan (COSMIC TOP SECRET) asiakirjoja, joita ei pääsääntöisesti luovuteta jäsenvaltioiden ulkopuolisille tahoille.

Naton turvallisuustoimisto teki Suomeen 3.-6.5.2022 tarkastusvierailun, jossa arvioitiin Naton turvallisuusluokitellun tiedon suojaamista. Tarkastuksen johtopäätösten mukaan viranomaisten tulee arvioida ja tarvittavilta osin lisätä Naton luokitellun tiedon suojaamista koskevia resursseja. Tämä koskee nimenomaisesti kansallista turvallisuusviranomaista ja henkilöturvallisuusselvityksiä, kirjaamohenkilökuntaa, tietojärjestelmien ja sähköisten käsittely-ympäristöjen hyväksymisprosessia, toimitilaturvallisuutta ja yritysturvallisuutta. Pääesikunnassa on tunnistettu tarve vahvistaa asiantuntijaresursseja edellä mainituilla osa-alueilla. Puolustusvoimissa kasvaa tarve perusmuotoisille ja erityisesti laajoille henkilöturvallisuusselvityksille. Myös tarve Pääesikunnan laatimille yritysturvallisuusselvityksille voi kasvaa. Nämä lisäävät Pääesikunnan henkilöresursointitarvetta.

Nato-jäsenyys tulee lisäämään Naton turvallisuusluokitellun tiedon määrää Suomessa. Nato suosittelee turvallisuusluokiteltujen tietojen suojaamisessa ensisijaisesti sähköistä tiedonsiirtoa ja käsittelyä. Sähköinen tiedonsiirto on myös kansallisesta näkökulmasta operatiivisen yhteistyön ja päätöksenteon oikea-aikaisuuden varmistamiseksi välttämätöntä. Sähköisten tietojenkäsittely-ympäristöjen toteuttamisessa tulee ottaa huomioon eri ministeriöiden, Suomen ulkomaan edustustojen, tasavallan presidentin kanslian sekä virastojen ja erityisesti Puolustusvoimien tarpeet. Asiakirjajakelut tulevat kohdentumaan eri hallinnonaloille, mutta erityisesti määrän kasvu näkyy Puolustusvoimissa sekä ulko- ja puolustusministeriöissä. Sellaisen kansallisen TLII-ympäristön kehittäminen, joka on hyväksytty myös NATO SECRET -tason turvallisuusluokitellun tiedon käsittelyyn, on välttämätöntä mahdollisimman nopealla aikataululla. Sähköisen käsittelyympäristön toteutus nojaa osin päätökseen, kuinka rekisteritoiminnot kansallisesti toteutetaan. Sähköisen tietojenkäsittely-ympäristön toteutusmallit ja rekisteröintitoiminnot ovat tällä hetkellä kansallisessa harkinnassa.

Naton tietoturvallisuusvaatimusten mukaan turvallisuusluokiteltua tietoa NATO CONFIDENTIAL tasolta alkaen voi käsitellä ja säilyttää vain kulunvalvonnan piirissä olevalla ja fyysisesti

suojatulla viranomaisen hyväksymällä turva-alueella. NATO RESTRICTED tason tietoa on käsiteltävä viranomaisen hyväksymällä hallinnollisella alueella. Fyysisten käsittely-ympäristöjen toteuttamiseen kohdistuu merkittäviä kustannuksia koko valtionhallinnossa.

Naton turvallisuussääntöjen mukaan kaikkien Naton turvallisuusluokiteltua tietoa käsittelevien tietojärjestelmien on läpikäytävä hyväksymisprosessi. Tämä koskee Naton Suomelle toimittamia järjestelmiä ja Suomen kansallisia järjestelmiä, joissa käsitellään Naton turvallisuusluokiteltua tietoa. Naton toimittamien järjestelmien osalta Liikenne- ja viestintävirasto vastaa järjestelmän kansallisen käyttöpisteen akkreditoinnista ja toimittaa sitä koskevan lausunnon (Statement of Compliance) Naton turvallisuushyväksyntälautakunnalle. Naton turvallisuusluokiteltua tietoa käsittelevien kansallisten tietojärjestelmien hyväksyntäprosessi koostuu riskiarvioinnista, järjestelmäkohtaisten vaatimusten määrittelystä, tarkastuksesta ja akkreditoinnista, jäännösriskin hyväksymisestä annetun akkreditointilausunnon pohjalta sekä käyttöluvan antamisesta. Akkreditointilausunto on voimassa kolme vuotta. Naton turvallisuusluokiteltua tietoa käsittelevien järjestelmien tarkastus- ja hyväksyntätyön on arvioitu edellyttävän Liikenne- ja viestintävirastossa pysyvästi lisäresursointitarpeita.

Kansallinen tietojärjestelmäkokonaisuus Naton turvallisuusluokiteltujen tietojen käsittelyyn tulee suunnitella niin, että se täyttää Naton tietojärjestelmäturvallisuutta koskevat vaatimukset. Liikenne- ja viestintävirasto tarjoaa viranomaisille neuvontaa järjestelmien turvallisuusvaatimusten suunnittelussa, mikä tukee hyväksyntäprosessin sujuvaa etenemistä. Kansallisen järjestelmäkokonaisuuden suunnittelun tuki ja arviointiprosessin tehokkaan toteuttamisen varmistaminen edellyttävät virastossa lisäresursointia.

Eduskunnan tiedusteluvaliokunta on kiinnittänyt hallituksen esitystä HE 315/2022 vp käsitellessään huomiota tieto- ja tilaturvallisuudesta huolehtimiseksi vaadittavien toimenpiteiden resursoinnin kannalta kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa tarkoitettujen kansallisen turvallisuusviranomaisen ja määrättyjen turvallisuusviranomaisten tehtävien lisääntymiseen (TiVL 1/2022 vp, s. 3).

6.3 Vaikutukset elinkeinoelämään

Tietoturvallisuussopimus antaa suomalaisille yrityksille mahdollisuuden tulla valituksi Naton järjestämään tai muutoin organisoimaan hankkeeseen taikka toisessa valtiossa järjestettävään hankintakilpailuun, joka edellyttää Naton turvallisuusluokiteltujen tietojen käsittelyä.

Turvallisuusluokiteltua tietoa sisältäviä hankkeita toteutetaan erityisesti puolustusteollisuuden, turvallisuuden, ydinvoiman, informaatioteknologian ja muun korkean teknologian aloilla sekä tieteen- ja tutkimuksen aloilla. Ilman tietoturvallisuussopimusta suomalaiset yritykset jäisivät Natossa toteutettavien turvallisuusluokiteltua tietoa sisältävien hankkeiden ulkopuolelle. Hankkeeseen valituksi tuleminen voi sopimuksen perusteella edellyttää yritykseltä turvallisuusselvityslain (46 §) mukaista yritysturvallisuusselvitystodistusta. Yritykseltä peritään turvallisuusselvityslain nojalla tehdyistä yritysturvallisuusselvityksistä maksu noudattaen, mitä valtion maksuperustelaissa (150/1992) säädetään.

Sopimuksen tarkoitus on mahdollistaa hankkeisiin osallistuminen ja näin parantaa suomalaisten yritysten kilpailukykyä ja ulkomaankauppaa.

7 Lausuntopalaute

Luonnos hallituksen esitykseksi on ollut lausuntokierroksella 24.3.–21.4.2023. Lausuntoja pyydettiin 24 taholta. Lausuntoja annettiin yhteensä x kappaletta. Lausuntopyyntö ja lausunnot ovat saatavilla osoitteessa valtioneuvosto.fi/hankkeet hankenumerolla UM001:00/2023.

8 Tietoturvallisuudesta Pohjois-Atlantin sopimuksen osapuolten välillä tehdyn sopimuksen määräykset ja niiden suhde Suomen lainsäädäntöön

8.1 Sopimus Pohjois-Atlantin sopimuksen osapuolten välillä tietoturvallisuudesta

Johdanto. Sopimuksen johdannossa vahvistetaan se, että tehokas poliittinen neuvottelu, yhteistyö ja suunnittelu puolustusasioissa Pohjois-Atlantin sopimuksen tavoitteiden saavuttamiseksi edellyttävät turvallisuusluokitellun tiedon vaihtamista osapuolten välillä. Johdannossa tunnistetaan myös se, että tiedonvaihto Pohjois-Atlantin sopimuksen osapuolten välillä edellyttää määräyksiä turvallisuusluokitellun tiedon vastavuoroisesta suojaamisesta ja turvaamisesta. Tällaisille turvallisuusvaatimuksille ja menettelyille tarvitaan yleiset puitteet, joista sopimuksessa sovitaan.

1 artikla. Sopimuksen 1 artiklan i kohdan mukaan osapuolet sitoutuvat suojaamaan ja turvaamaan sopimuksen I liitteessä tarkemmin määritellyn turvallisuusluokitellun tiedon, jonka alkuperäinen luovuttaja on Nato tai jonka jäsenvaltio toimittaa Natolle sekä jäsenvaltioiden turvallisuusluokitelluksi merkityn turvallisuusluokitellun tiedon, joka toimitetaan toiselle jäsenvaltiolle Naton ohjelman, hankkeen tai sopimuksen tueksi.

Sopimus soveltuu siten Suomen ja Naton välillä vaihdettavan turvallisuusluokitellun tiedon lisäksi jäsenvaltioiden välillä vaihdettavaan turvallisuusluokiteltuun tietoon, joka toimitetaan Naton ohjelman, hankkeen tai sopimuksen tueksi. Sopimuksen soveltaminen jäsenvaltioiden välillä ei siten edellytä muodollista Naton yhteistyötä vaan sitä sovelletaan myös jäsenvaltioiden väliseen kansainväliseen yhteistoimintaan, jolla tuetaan Naton toimintaa. Pohjois-Atlantin sopimuksen 3 artiklan mukaisesti osapuolet ylläpitävät ja kehittävät yhdessä ja erikseen, jatkuvan ja tehokkaan oman valmistautumisen ja keskinäisen avun pohjalta, kansallista ja yhteistä kykyään puolustautua aseellisia hyökkäyksiä vastaan. Artiklan mukaista yhteistoimintaa voidaan toteuttaa jäsenvaltioiden välillä ilman Naton muodollista yhteistoiminnan muotoa tai Naton toimielinten osallistumista. Naton tietoturvallisuussopimusta sovelletaan myös tällaisessa kahden- tai monenvälisessä yhteistoiminnassa vaihdettavaan jäsenvaltioiden kansalliseen turvallisuusluokiteltuun tietoon. Usein myös tällaista yhteistoimintaa määrittävissä kansainvälisissä sopimusasiakirjoissa viitataan Naton tietoturvallisuutta koskeviin vaatimuksiin tai niiden suojaamisen tasoon. Sopimus voi edesauttaa lisäksi kansallisen turvallisuusluokitellun tiedon vaihtoa Naton jäsenvaltioiden kesken muissakin tilanteissa, jos kahdenvälistä tietoturvallisuutta koskevaa valtiosopimusta ei ole olemassa ja jos molemmat osapuolet katsovat sen siihen soveltuvan.

Artiklan ii kohdan mukaan osapuolet säilyttävät i kohdassa tarkoitetun tiedon turvallisuusluokituksen ja pyrkivät kaikin keinoin turvaamaan tiedon sen mukaisesti. Artiklan iii kohdan mukaan turvallisuusluokiteltua tietoa ei käytetä muihin kuin Pohjois-Atlantin sopimuksessa ja siihen liittyvissä päätöksissä ja päätöslauselmissa määrättyihin tarkoituksiin. Määräys sisältää kansainvälisiin tietoturvallisuussopimuksiin tyypillisesti kuuluvan käyttötarkoitussidonnaisuusperiaatteen. Artiklan iv kohdan mukaan sopimuksen osapuolet eivät ilmaise tällaista tietoa Natoon kuulumattomille osapuolille ilman tiedon alkuperäisen luovuttajan suostumusta.

Sopimukseen sovellettaisiin sopimuksen voimaan saattamisen jälkeen kansainvälisistä tietoturvallisuusvelvoitteista annettua lakia, jonka 3 luvun määräykset tietoturvallisuustoimenpiteistä sisältävät 1 artiklan määräysten täytäntöön panemiseksi tarvittavat säännökset.

2 artikla. Artiklan mukaan osapuolet varmistavat kansallisen turvallisuusviranomaisen perustamisen Naton toimintaa varten toteuttamaan suojaavia turvatoimia. Osapuolet laativat ja panevat täytäntöön turvallisuusvaatimuksia, joilla varmistetaan turvallisuusluokitellun tiedon yhteinen suojauksen taso. Näitä turvallisuusvaatimuksia selostetaan tarkemmin jäljempänä jaksossa 8.2.

Turvallisuusluokitellun tiedon käsittelylle asetetuista vaatimuksista säädetään kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa, julkisen hallinnon tiedonhallinnasta annetussa laissa ja turvallisuusluokitteluasetuksessa. Turvallisuusluokitteluasetusta sovelletaan Naton turvallisuusluokiteltavien asiakirjojen käsittelyyn, jollei kansainvälisestä tietoturvallisuusvelvoitteesta muuta johdu.

Kansainvälisitä tietoturvallisuusvelvoitteista annetun lain 3 luvun säännökset sisältävät keskeiset laintasoiset tietoturvallisuustoimenpiteet: salassapito ja tietojen käyttö (6 §), vaitiolovelvollisuus ja hyväksikäyttökielto (7 §), turvallisuusluokan merkitseminen (8 §), turvallisuusluokkaa vastaavat käsittelyvaatimukset (9 §) ja tiloihin liittyvät turvallisuusvaatimukset (10 §).

Turvallisuusluokitteluasetuksen 6–15 §:ssä säädetään turvallisuusluokiteltujen asiakirjojen käsittelyssä toteutettavista tietoturvallisuustoimenpiteistä, jotka liittyvät kansainvälisiä tietoturvallisuusvelvoitteita ja asiakirjan elinkaarta mukaillen asiakirjan antamisen edellytyksiin (6 §), monitasoiseen suojaukseen (7 §), käsittelyoikeuden antamiseen ja niiden luettelointiin (8 §), turvallisuusalueisiin eli toimitilaturvallisuuteen (9 §), asiakirjan käsittelyn ja tietojärjestelmien suojaamiseen turvallisuusalueiden avulla (10 §), tietojärjestelmiä ja tietoliikennejärjestelyjä koskeviin vaatimuksiin (11 §), asiakirjan siirtämiseen tietoverkon kautta (12 §), asiakirjan kuljettamiseen (13 §), asiakirjan käsittelyn seuraamiseen (14 §) ja asiakirjan tuhoamiseen (15 §).

Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 4 §:n mukaan ulkoministeriö toimii kansainvälisten tietoturvallisuusvelvoitteiden toteuttamisessa Suomen kansallisena turvallisuusviranomaisena. Puolustusministeriö, Pääesikunta, Suojelupoliisi ja Liikenne- ja viestintävirasto toimivat määrättyinä turvallisuusviranomaisina. Kansallisen turvallisuusviranomaisen tehtävänä on erityisesti ohjata ja valvoa, että tässä laissa tarkoitetut erityissuojattavat tietoaineistot suojataan ja niitä käsitellään asianmukaisesti.

Määrätyt turvallisuusviranomaiset huolehtivat niille kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa säädetyistä ja muista niille kansainvälisistä tietoturvallisuusvelvoitteista johtuvista tehtävistä. Puolustusministeriö, Pääesikunta ja Suojelupoliisi toimivat kansallisen turvallisuusviranomaisen asiantuntijoina henkilöstö-, yritys- ja toimitilaturvallisuutta koskevissa asioissa sekä Liikenne- ja viestintävirasto tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuutta koskevissa asioissa.

Kansallinen turvallisuusviranomainen on julkaissut Katakri-työkalun, johon on koottu kansallisiin säädöksiin ja kansainvälisiin velvoitteisiin perustuvat vähimmäisvaatimukset. Katakri on viranomaisten tietoturvallisuuden auditointityökalu, jota voidaan käyttää arvioitaessa kohdeorganisaation kykyä suojata kansallista tai kansainvälistä turvallisuusluokiteltua tietoa. Katakri itsessään ei aseta tietoturvallisuudelle ehdottomia vaatimuksia, vaan siihen kootut vaatimukset perustuvat voimassa olevaan lainsäädäntöön ja Suomea sitoviin kansainvälisiin tietoturvallisuusvelvoitteisiin. Vaatimukset on kuvattu siten, että ne mahdollistavat erilaisia toteutustapoja. Lisätietokenttiin on tulkinnan tueksi koottu toteutusesimerkkejä, joissa kuvatuilla menettelyillä

voidaan useimmissa ympäristöissä saavuttaa hyväksyttävä suojauksen vähimmäistaso. Toteutusesimerkit eivät ole sitovia ja ne ovat korvattavissa myös muilla vastaavan tasoisilla suojauksilla.

Kansallinen turvallisuusviranomainen yhteistyössä määrättyjen turvallisuusviranomaisten kanssa on julkaisemassa Katakria täydentävän Nato-liitteen tukemaan niitä julkishallinnon ja elinkeinoelämän organisaatioita, jotka tulevat käsittelemään Naton turvallisuusluokiteltua tietoa. Liite perustuu Suomelle vuoden 2022 aikana luovutettuihin Naton tarkentaviin turvallisuussääntöihin ja -ohjeisiin, joista on tehty vertailuanalyysi Katakriin. Liite ei tuo merkittäviä muutoksia Katakrin sisältöön tai sen soveltamiseen, vaan pyrkii esittämään ainoastaan huomionarvoiset eroavaisuudet kansallisten ja Naton turvallisuusvaatimusten välillä.

Voimassaolevan turvallisuusluokitteluasetuksen mukaisessa turvallisuusaluejaossa ja asiakirjojen käsittelysäännöissä (9-10 §) on otettu huomioon Euroopan unionin neuvoston turvallisuussäännöt, joiden mukaan turvallisuusluokiteltuja tietoja, jotka kuuluvat CONFIDENTIAL- (turvallisuusluokka III) tai SECRET- (turvallisuusluokka II) turvallisuusluokkaan, voidaan käsitellä hallinnollisella alueella, jos pääsy tietoihin on suojattu sivullisilta. Naton turvallisuussäännöstö mahdollistaa kuitenkin enintään NATO RESTRICTED- (turvallisuusluokka IV) turvallisuusluokan tiedon käsittelyn hallinnollisella alueella. Tämä käsittelysääntöjen ero ja tarvittavat rinnastukset on esitetty Katakrin Nato-liitteessä. Turvallisuusluokitteluasetusta sovelletaan Suomessa niin kansallisen kuin kansainvälisenkin turvallisuusluokitellun tiedon käsittelyyn, jollei kansainvälisestä tietoturvallisuusvelvoitteesta muuta johdu. Naton turvallisuussäännöstössä kuvatut vähimmäisvaatimukset ovat tällainen Suomea sitova kansainvälinen velvoite, jonka määräykset tulevat sovellettavaksi Natolta peräisin olevan tiedon käsittelyssä.

3 artikla. Artiklan 1 kohdan mukaan osapuolet sitoutuvat varmistamaan, että kaikista niiden kansalaisista, jotka virallisia tehtäviään hoitaessaan tarvitsevat tai saattavat saada pääsyn turvallisuusluokkaan CONFIDENTIAL ja sitä ylempiin turvallisuusluokkiin kuuluvaan tietoon, tehdään asianmukaisesti turvallisuusselvitys ennen kuin he ottavat tehtävänsä vastaan. Naton turvallisuussääntöjen mukaan poikkeuksen PSC-vaatimuksesta muodostavat valtion ylimpien tehtävien haltijat (valtion- ja hallitusten päämiehet, ministerit, kansanedustajat sekä oikeuslaitoksen jäsenet), joiden osalta pääsy Naton turvallisuusluokiteltuun tietoon perustuu kansallisiin säädöksiin ja määräyksiin. Viimeksi mainittuja henkilöitä on kuitenkin ohjeistettava tiedon käsittelyyn liittyvistä turvallisuusvelvoitteista ja heillä tulee olla tiedon käsittelyyn tiedonsaantitarve.

Artiklan 2 kohta sisältää turvallisuusselvitysmenettelyitä koskevan vaatimuksen. Niillä on pystyttävä selvittämään, voiko henkilö hänen lojaliteettinsa ja luotettavuutensa huomioon ottaen saada pääsyn turvallisuusluokiteltuun tietoon ilman, että siitä aiheutuu turvallisuusriski, jota ei voida hyväksyä.

Artiklan 3 kohta edellyttää, että osapuolet tekevät pyydettäessä yhteistyötä muiden osapuolten kanssa niiden turvallisuusselvitysmenettelyjä suoritettaessa.

Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 11 §:n mukaan kansainvälisessä tietoturvallisuusvelvoitteessa edellytetty henkilöturvallisuusselvitys laaditaan siten kuin turvallisuusselvityslaissa säädetään. Henkilöturvallisuusselvitystodistuksen antaa kuitenkin kansallinen turvallisuusviranomainen, jollei eritvisistä svistä muuta johdu. Turvallisuusselvityslain 26 §:ssä säädetään tiedon hankkimisesta ulkomaan viranomaisen rekistereistä. Kansainvälisistä turvallisuusvelvoitteista annetun lain 17 §:ssä säädetään kansainvälisen tietoturvallisuusvelvoitteen toteuttamiseksi välttämättömien asiakirjojen ja tietojen luovuttamisesta tietoturvallisuussopimuksen osapuolelle.

4 artikla. Artiklan mukaan Naton pääsihteerin tulee varmistaa, että vastaavasti Nato soveltaa sopimuksen turvallisuusluokitellun tiedon suojaamista koskevia määräyksiä. Asiaa koskeva tarkennus sisältyy sopimuksen III liitteeseen.

Natossa on hyväksytty tässä artiklassa tarkoitettuja yksityiskohtaisia määräyksiä, joita sovelletaan sekä jäsenvaltioiden että Naton toimintaan. Naton puolella Naton turvallisuustoimisto (Nato Office of Security, NOS) koordinoi, valvoo ja panee täytäntöön Naton turvallisuussäännöstön (Nato Security Policy).

5 artikla. Artiklan mukaan sopimus ei millään tavoin estä osapuolia tekemästä muita sopimuksia, jotka liittyvät niiden luovuttaman turvallisuusluokitellun tiedon vaihtamiseen eivätkä vaikuta tämän sopimuksen soveltamisalaan.

Suomella on tällä hetkellä kahdenvälisiä tietoturvallisuussopimuksia 20 valtion kanssa sekä Pohjoismaiden, Euroopan unionin jäsenvaltioiden, Euroopan avaruusjärjestön, Euroopan puolustusmateriaalijärjestö OCCARin sekä Pohjois-Atlantin liiton kanssa. Naton kanssa tehty aiempi sopimus ja hallinnollinen järjestely korvautuvat nyt hyväksyttävällä sopimuksella.

6 artikla. Sopimus on ollut avoinna allekirjoittamista varten Naton silloisille jäsenvaltioille, joiden ratifioimis- tai hyväksymiskirjat on tullut tallettaa Amerikan yhdysvaltojen hallituksen huostaan. Artiklan b kohdan mukaan sopimus on tullut voimaan kolmenkymmenen päivän kuluttua päivästä, jona kaksi allekirjoittajavaltiota on tallettanut ratifioimis- tai hyväksymiskirjansa. Sopimus on tullut määräyksen mukaisesti kansainvälisesti voimaan 16.8.1998. Sen jälkeen sopimus on tullut voimaan kunkin muun allekirjoittajavaltion osalta kolmenkymmenen päivän kuluttua kunkin valtion ratifioimis- tai hyväksymiskirjan tallettamisesta.

Artiklan c kohdan mukaan sopimus on korvannut Pohjois-Atlantin neuvoston 1952 hyväksymän asiakirjan D.C.2/7 liitteessä olevan lisäyksen liitteessä A (1 kohta) 19 päivänä huhtikuuta 1952 ja joka myöhemmin sisällytettiin Pohjois-Atlantin neuvoston 2 päivänä maaliskuuta 1955 hyväksymän asiakirjan C-M (55) 15 (final) liitteeseen A.

7 artikla. Artikla sisältää Suomeen soveltuvan määräyksen tietoturvallisuussopimukseen liittymisestä. Sopimus on avoinna liittymistä varten Pohjois-Atlantin sopimuksen uudelle osapuolelle sen valtiosäännön mukaisten menettelyjen mukaisesti. Liittymiskirja talletetaan Amerikan yhdysvaltojen hallituksen huostaan. Sopimus tulee voimaan kunkin liittyvän valtion osalta kolmenkymmenen päivän kuluttua sen liittymiskirjan tallettamispäivästä. Suomi on liittymisneuvotteluissa sitoutunut liittymään tietoturvallisuussopimukseen 12 kuukauden kuluessa siitä, kun Suomi on tallettanut Pohjois-Atlantin sopimusta koskevan liittymiskirjansa

8 artikla. Amerikan yhdysvaltojen hallitus ilmoittaa muiden osapuolten hallituksille kunkin ratifioimis-, hyväksymis- tai liittymiskirjan tallettamisesta.

9 artikla. Artikla sisältää sopimuksen irtisanomista koskevat määräykset. Osapuoli voi irtisanoa sopimuksen antamalla kirjallisen irtisanomisilmoituksen tallettajalle, joka ilmoittaa irtisanomisilmoituksesta kaikille muille osapuolille. Irtisanominen tulee voimaan vuoden kuluttua siitä, kun tallettaja on vastaanottanut ilmoituksen, mutta ei vaikuta niihin velvoitteisiin, oikeuksiin tai valtaoikeuksiin, joita osapuolet ovat aiemmin sopineet tai saaneet tämän sopimuksen määräysten perusteella.

Todistusvoimaiset tekstit. Sopimuksen todistusvoimaiset kielet ovat englanti ja ranska. Sopimuksen tallettajana toimii Amerikan yhdysvaltojen hallitus.

Liite I. Sopimuksen liitteet muodostavat sopimuksen erottamattoman osan. Liitteessä I määritellään Naton turvallisuusluokiteltu tieto. Liitteen a kohdan mukaan "tieto" tarkoittaa missä tahansa muodossa välitettävää tietoa. Sen b kohdan mukaan turvallisuusluokiteltu tieto tarkoittaa tietoa tai aineistoa, jonka katsotaan edellyttävän suojaamista luvattomalta paljastamiselta ja joka on turvallisuusluokituksella osoitettu sellaiseksi. Liitteen c kohdan mukaan ”aineisto” sisältää asiakirjat ja myös valmistetut ja valmisteilla olevat koneet, laitteet ja aseet. Liitteen d kohdan mukaan ”asiakirja” tarkoittaa mitä tahansa tallennettua tietoa riippumatta sen fyysisestä muodosta tai ominaisuuksista, mukaan lukien kirjalliset ja painotuotteet; tietojenkäsittelyssä käytettävät kortit ja nauhat; kartat, kaaviot, valokuvat, maalaukset, piirustukset, kaiverrukset, luonnokset, työmuistiinpanot ja –paperit, hiilipaperikopiot ja värinauhat; millä tahansa keinolla tai menettelyllä tehdyt jäljennökset; kaikenlaiset ääni-, puhe- ja magneettitallenteet sekä elektroniset, optiset ja videotallenteet; kannettavat atk-laitteet, joissa on kiinteät tallennusvälineet, ja irrotettavat tietokoneen tallennusvälineet, mutta ei rajoittuen näihin. Viranomaisen asiakirja on määritelty kansallisessa lainsäädännössä julkisuuslain 5 §:ssä.

Liite II. Liitteessä määritellään, mitä Natolla tässä sopimuksessa tarkoitetaan. ”Nato” tarkoittaa Pohjois-Atlantin liittoa ja niitä elimiä, joihin sovelletaan joko Ottawassa 20 päivänä syyskuuta 1951 allekirjoitettua sopimusta Pohjois-Atlantin liiton, kansallisten edustajien ja kansainvälisen henkilöstön asemasta tai Pariisissa 28 päivänä elokuuta 1952 allekirjoitettua pöytäkirjaa Pohjois-Atlantin sopimuksen mukaisesti perustettujen kansainvälisten sotilasesikuntien asemasta.

Liite III. Liite sisältää sopimuksen 4 artiklaa täydentävän määräyksen, jonka mukaan sotilaskomentajien kanssa neuvotellaan heidän valtaoikeuksiensa kunnioittamiseksi. Sotilaskomitea vastaa kaikista Naton sotilasrakenteen turvallisuusasioista ja sen alaisuuteen perustettujen Naton sotilaselinten johtajat vastaavat kaikista organisaatioidensa turvallisuusasioita. Turvallisuussääntöjen mukaan turvallisuustoimiston tulee esimerkiksi tiedottaa sotilaskomitean puheenjohtajalle Naton turvallisuustilanteesta sekä edistymisestä turvallisuutta koskevien NAC:n päätösten täytäntöönpanossa.

8.2 Naton tietoturvallisuutta koskevat vaatimukset ja osa-alueet

Naton turvallisuustoiminta perustuu Naton sisäisesti hyväksyttyyn turvallisuussäännöstöön (Nato Security Policy) ja sen pohjalle rakentuviin jäsenvaltioiden turvallisuusmenettelyihin. Naton osalta tietoturvallisuussopimuksen 2 artiklassa tarkoitetun yhteisen suojauksen tason perusperiaatteet ja vähimmäisvaatimukset on vahvistettu Naton asiakirjassa C-M(2002)49-REV1, ”Security within the North Atlantic Treaty Organization” (jäljempänä Naton turvallisuussäännöt), sitä tukevissa direktiiveissä (*directives*), suuntaviivoissa (*guidelines)* sekä tulkintaohjeissa (*supporting documents*). Turvallisuussääntöjen mukaan jäsenvaltiot varmistavat säännöissä määrättyjen perusperiaatteiden ja vähimmäisvaatimusten soveltamisen, jotta Naton turvallisuusluokitellun tiedon luottamuksellisuuden, eheyden ja käytettävyyden säilyminen turvataan.

Turvallisuussäännöstö asettaa turvallisuuden perusperiaatteet ja vähimmäisvaatimukset, jotta Naton turvallisuusluokitellulle tiedolle annetaan todennetusti vaatimustenmukainen suoja jäsenmaissa ja Naton elimissä. Turvallisuussäännöstö muodostaa tietoturvallisuussopimuksen täytäntöönpanoa koskevan laajan ja yksityiskohtaisen kokonaisuuden, joka ei ole kuitenkaan osa sopimusta.

Osapuolet arvioivat ja päivittävät Naton turvallisuussäännöstöä eri kokoonpanoissa. Naton tietoturvallisuutta koskevia asioita käsitellään Naton turvallisuuskomitean turvallisuuspolitiikkakokoonpanossa. Komitean sihteeristönä toimii Naton turvallisuustoimisto (NOS (*NATO Office of Security*), joka myös asettaa komitean puheenjohtajan. Komitean jäsenistö muodostuu jäsen-

valtioiden kansallisista (NSA; National Security Authority) ja/tai määrätyistä turvallisuusviranomaisista (DSA; Designated Security Authority). Suomi on osallistunut komitean työhön vuodesta 2011 alkaen. Turvallisuuskomitealla on myös teknisen tietoturvallisuuden CISS-kokoonpano (NATO SC(CISS)). Naton sotilas- ja siviilielimet vastaavat toimialojensa turvallisuusasioista.

Naton turvallisuussäännöstön tietoturvallisuuden osa-alueet ovat henkilöstöturvallisuus, toimitilaturvallisuus, tietoaineistoturvallisuus, viestintä- ja tietojärjestelmien turvallisuus ja yritysturvallisuus. Toimenpiteet ulottuvat henkilöihin, järjestelmiin, tiloihin, infrastruktuuriin ja ympäristöön sekä tiedon käsittelyn kontrolleihin ja tiedonhallintaan. Näitä koskevat keskeiset turvallisuusvaatimukset sisältyvät Naton turvallisuussääntöjen C-M(2002)49-REV1 liitteisiin B-H, joiden sisältöä selostetaan alla.

Liite A - Pohjois-Atlantin sopimuksen osapuolten välillä tietoturvallisuudesta tehty sopimus

Turvallisuussääntöjen liite A sisältää varsinaisen tietoturvallisuussopimuksen tekstin, jonka sisältöä on selostettu edellä jaksossa 8.1.

Liite B – Perusperiaatteet, vähimmäisvaatimukset ja vastuut

Turvallisuussääntöjen liitteessä B kuvataan Naton turvallisuussääntöjen soveltamiseen liittyvät perusperiaatteet, vähimmäisvaatimukset sekä vastuut, joita soveltamalla Naton jäsenvaltiot ja Naton sotilas- ja siviilielimet varmistavat osapuolten kesken vaihdettavalle turvallisuusluokitellulle tiedolle yhteisen suojauksen tason.

Kuvatut perusperiaatteet ja vähimmäisvaatimukset liittyvät muun muassa turvallisuusluokitellun tiedon käsittelyoikeuksien rajaamiseen, sisäpiiriuhkien huomioimiseen osana turvallisuusmenettelyjä, turvallisuuskoulutuksen järjestämiseen, tietoturvaloukkauksia koskevaan ilmoitusvelvollisuuteen ja -menettelyyn sekä turvallisuusluokitellun tiedon alkuperäisen luovuttajan määräysvaltaan luovuttamansa tiedon osalta. Naton turvallisuusluokiteltua tietoa luovutetaan vakiintuneiden luovutusmenettelyjen ja –perusteiden mukaisesti ja tieto tulee suojata vähintään samantasoisesti kuin Naton turvallisuussäännöissä ja sitä tukevissa ohjeissa edellytetään.

Naton turvallisuusluokiteltua tietoa koskevat vähimmäisvaatimukset on ulotettava koskemaan kaikkia henkilöitä, joilla on pääsy turvallisuusluokiteltuun tietoon sekä kaikkia tiloja ja tietovälineitä, joissa tällaista tietoa käsitellään. Tällaista tietoa voidaan jakaa ainoastaan viralliseen tehtävään liittyvän tiedonsaantitarpeen perusteella. Turvallisuusluokan NATO CONFIDENTIAL ja tätä korkeammin luokiteltujen tietoaineistojen osalta edellytetään lisäksi, että tietoa käsittelevät henkilöt ovat asianmukaisesti turvallisuusselvitetty ja heille on annettu tieto käsittelyssä sovellettavista turvallisuusmenettelyistä. Turvallisuusluokitellun tiedon käsittelyedellytyksiä tulee arvioida myös turvallisuusselvitystodistuksen myöntämisen jälkeen erilaisten seurantatoimien kautta, minkä tarkoituksena on mahdollistaa tiedon vaarantumiseen liittyvän sisäpiiriuhkan hallinta.

Naton jäsenvaltion kansallinen turvallisuusviranomainen vastaa Naton turvallisuusluokitellun tiedon turvallisuudesta ja toimii Naton turvallisuustoimiston ensisijaisena yhteystahona kaikissa Naton turvallisuuteen liittyvissä asioissa. Tarvittaessa se voi ohjata Naton turvallisuustoimiston kääntymään myös muun toimivaltaisen turvallisuusviranomaisen puoleen. Kansallisen turvallisuusviranomaisen vastuulla on varmistaa Naton turvallisuusluokitellun tiedon turvallisuus sekä sotilas- että siviilialan virastoissa ja yksiköissä niin kotimaassa kuin ulkomaillakin. Sen vastuulla on varmistaa, että kaikissa kansallisissa organisaatioissa tehdään määräajoin asianmukai-

set tarkastukset sen arvioimiseksi, suojataanko Naton turvallisuusluokiteltua tietoa asianmukaisesti, ja että turvallisuusluokiteltua tietoa käsitteleville henkilöille on annettu henkilöturvallisuusselvitystodistus Naton turvallisuusperiaatteiden mukaisesti. Kansallinen turvallisuusviranomainen auktorisoi myös kansallisten COSMIC-keskusrekisterien perustamisen ja lakkauttamisen. Määrättyjen turvallisuusviranomaisten vastuulla on tiedottaa yrityksille ja muille yhteisölle kansallisista periaatteista kaikissa Naton yritysturvallisuuden periaatteita koskevissa asioissa ja antaa apua niiden soveltamisessa.

Naton jäsenvaltioiden kansallisten turvallisuusviranomaisten tai määrättyjen turvallisuusviranomaisten ja Naton sotilas- tai siviilielinten välinen Naton turvallisuusasia, jota ei voida ratkaista, tai Naton turvallisuusperiaatteiden toteuttamista tai tulkintaa koskeva asia saatetaan Naton turvallisuustoimiston ratkaistavaksi. Ratkaisemattomat erimielisyydet Naton turvallisuustoimisto antaa Naton turvallisuuskomitean käsiteltäväksi.

Naton jäsenvaltioiden ja Naton sotilas- ja siviilielinten ehdotukset Naton turvallisuusperiaatteiden muuttamiseksi annetaan ensisijaisesti Naton turvallisuustoimiston käsiteltäväksi. Naton turvallisuustoimisto käsittelee ehdotukset ja esittää ne tarvittaessa Naton turvallisuuskomitealle asian jatkokäsittelyä varten. Jäsenvaltioiden kansalliset turvallisuusviranomaiset sekä määrätyt turvallisuusviranomaiset voivat tämän estämättä tehdä virallisen ehdotuksen turvallisuusperiaatteiden muuttamisesta Naton turvallisuuskomitealle, jos ne niin tahtovat.

Liite C – Henkilöstöturvallisuus

Turvallisuussääntöjen henkilöstöturvallisuutta koskevat periaatteet ja vähimmäisvaatimukset on kuvattu turvallisuussääntöjen liitteessä C, jossa kuvattuja yleisperiaatteita tukee yksityiskohtaisempi Naton henkilöstöturvallisuutta koskeva direktiivi AC/35-D/2000. Henkilöstöturvallisuutta koskevat vaatimukset määrittelevät sitä, millä edellytyksillä henkilöille voidaan antaa pääsy Naton turvallisuusluokiteltuun tietoon.

Jäsenvaltion henkilöstöturvallisuusmenettelyjen tulee olla riittävät sen selvittämiseksi, voidaanko henkilölle myöntää hänen lojaalisuutensa, rehellisyytensä ja luotettavuutensa huomioon ottaen pääsy Naton turvallisuusluokiteltuun tietoon ilman, että siitä aiheutuva turvallisuusriski ylittää hyväksyttävän tason. Kaikki siviili- ja sotilashenkilöt, joiden tehtävät edellyttävät pääsyä turvallisuusluokan CONFIDENTIAL tai sitä ylempien turvallisuusluokkien tietoihin, on turvallisuusselvitettävä asianmukaisesti ja heillä tulee olla henkilöturvallisuusselvitystodistus (PSC), mikäli on saavutettu riittävä luottamuksen taso heidän kelpoisuudestaan saada pääsy tällaiseen tietoon. Poikkeuksen PSC-vaatimuksesta muodostavat valtion ylimpien tehtävien haltijat (valtion- ja hallitusten päämiehet, ministerit, kansanedustajat sekä oikeuslaitoksen jäsenet), joiden osalta pääsy Naton turvallisuusluokiteltuun tietoon perustuu kansallisiin säädöksiin ja määräyksiin. Viimeksi mainittuja henkilöitä on kuitenkin ohjeistettava tiedon käsittelyyn liittyvistä turvallisuusvelvoitteista ja heillä tulee olla tiedon käsittelyyn tiedonsaantitarve.

Naton jäsenvaltioiden sekä Naton siviili- ja sotilaselinten henkilöillä on pääsy vain sellaiseen Naton turvallisuusluokiteltuun tietoon, joihin heillä on tiedonsaantitarve (need-to-know). Kenelläkään ei ole oikeutta päästä Naton turvallisuusluokiteltuun tietoon yksinomaan henkilön aseman, viran tai henkilöturvallisuusselvitystodistuksen perusteella.

Kaikille henkilöille, joilla on pääsy Naton turvallisuusluokiteltuun tietoon tai joille on tehty henkilöturvallisuusselvitys turvallisuusluokitellun tiedon käsittelyä varten, tulee varmistaa asianmukaisen turvallisuuskoulutuksen järjestäminen. Tällaista tietoa käsitteleville henkilöille on ohjeistettava tiedon käsittelyyn liittyvistä turvallisuusmenettelyistä ja heidän turvallisuusvelvoitteistaan sekä säännöllisin väliajoin muistutettava myös erilaisista turvallisuusuhkista, joita

tiedon käsittelyyn liittyy. Kaikkien turvallisuusselvitettyjen henkilöiden on vakuutettava ymmärtävänsä täysin vastuunsa ja heihin mahdollisesti kohdistuvat seuraukset, mikäli Naton turvallisuusluokiteltua tietoa joutuu luvattomiin käsiin joko tahallisesti tai huolimattomuudesta.

Kansallisten turvallisuusviranomaisten ja määrättyjen turvallisuusviranomaisten tai muiden toimivaltaisten turvallisuusviranomaisten, Naton jäsenvaltioiden ja Naton siviili- tai sotilaselinten päälliköiden yksityiskohtaiset vastuut on määritelty henkilöstöturvallisuutta koskevassa direktiivissä (AC/35-D/2000).

Liite D – Toimitilaturvallisuus

Turvallisuussääntöjen liitteessä D kuvataan toimitilaturvallisuutta koskevat periaatteet ja vähimmäisvaatimukset Naton turvallisuusluokitellun tiedon suojaamiseksi. Lisätietoja toimitilaturvallisuuteen liittyvistä yksityiskohtaisista vaatimuksista löytyy Naton turvallisuusperiaatteita tukevasta toimitilaturvallisuutta koskevasta direktiivistä (AC/35-D/2001).

Naton jäsenvaltioiden on laadittava aktiivisia ja passiivisia turvallisuustoimia sisältävät toimitilaturvallisuuden ohjelmat, joilla saavutetaan yhteinen toimitilaturvallisuuden taso, joka vastaa arvioita suojattavan tiedon uhkista, haavoittuvuuksista, turvallisuusluokituksesta ja määrästä. Kaikki kohteet, rakennukset, tilat ja muut alueet, joissa Naton turvallisuusluokiteltua tietoa käsitellään tai siitä keskustellaan, on suojattava asianmukaisin fyysisin turvallisuustoimenpitein. Näiden turvallisuustoimenpiteiden tarkoituksena on estää tunkeutuminen, ehkäistä, estää ja havaita sisäpiiriuhkan toimet, mahdollistaa henkilöstön erottelu ja pääsy Naton turvallisuusluokiteltuun tietoon heidän henkilöturvallisuusselvitystodistuksen ja tiedonsaantitarpeen perusteella sekä mahdollistaa kaikkien tietoturvapoikkeamien havaitseminen ja niihin puuttuminen mahdollisimman nopeasti.

Toimitilaturvallisuuden ohjelmien on perustuttava monitasoisen suojaamisen periaatteeseen, jossa käytetään asianmukaista yhdistelmää toisiaan täydentäviä fyysisiä turvallisuustoimenpiteitä, jotka tarjoavat sellaisen suojan tason, joka täyttää organisaation ja sen tietojen kriittisyyteen ja haavoittuvuuteen liittyvät vaatimukset. Fyysisiä turvallisuustoimenpiteitä tukemassa on oltavat asianmukaiset henkilöstö-, tieto- sekä viestintä- ja tietojärjestelmäturvallisuuden toimenpiteet.

Pysyvät tai tilapäiset alueet, joissa NATO CONFIDENTIAL tason turvallisuusluokiteltua tietoa säilytetään, käsitellään tai joissa siitä keskustellaan, on järjestettävä ja muodostettava siten, että ne vastaavat Naton I–luokan tai Naton II-luokan turva-alueen vaatimuksia. Naton I- tai II-luokan turva-alueiden ympärille tai niille johtavalle alueelle on perustettava hallinnollinen vyöhyke. Hallinnollisilla vyöhykkeillä sallitaan vain turvallisuusluokan NATO RESTRICTED tiedon säilyttäminen, käsittely tai siitä keskusteleminen. Tällaisilla alueilla on oltava selkeästi määritetyt rajat, joilla on mahdollisuus tarkastaa henkilöt ja ajoneuvot.

Teknisesti suojatut turva-alueet ovat joko kiinteitä tai tilapäisiä alueita, jotka ovat nimenomaisesti tunnistettu teknisiltä hyökkäyksiltä ja salakuuntelulta suojattaviksi alueiksi. Tällaisilla alueilla on tehtävä säännöllisiä fyysisiä ja teknisiä tarkastuksia ja niihin pääsyä on valvottava tarkasti.

Turvallisuusluokkiin COSMIC TOP SECRET, NATO SECRET ja NATO CONFIDENTIAL kuuluvat tiedot on säilytettävä luokan I tai II turva-alueella noudattaen Naton turvallisuussäännöissä määriteltyjä tarkempia ehtoja. Turvallisuusluokkaan NATO RESTRICTED kuuluva tieto on säilytettävä lukitussa kaapissa tai toimistokalusteessa hallinnollisella alueella tai luokan I tai II turva-alueella.

Naton jäsenvaltioiden tulee käyttää vain sellaisia laitteita, jotka asianomainen turvallisuusviranomainen on hyväksynyt Naton turvallisuusluokitellun tiedon säilyttämiseen.

Liite E – Naton turvallisuusluokitellun tiedon turvallisuus

Turvallisuussääntöjen liitteessä E kuvataan Naton turvallisuusluokitellun tiedon turvallisuutta koskevat periaatteet ja vähimmäisvaatimukset. Tietoturvallisuus on yleisten suojaustoimenpiteiden ja –menettelyjen soveltamista turvallisuusluokitellun tiedon katoamisen tai vaarantumisen estämiseksi, havaitsemiseksi ja korjaamiseksi.

Luovuttaja vastaa turvallisuusluokitellun tiedon turvallisuusluokan määrittämisestä. Keskeisen periaatteen mukaan turvallisuusluokkaa ei saa vaihtaa, alentaa eikä poistaa ilman alkuperäisen luovuttajan suostumusta. Liitteessä E luetellaan Naton turvallisuusluokat, niistä käytettävät lyhenteet sekä määritellään merkitykset seuraavasti:

COSMIC TOP SECRET (CTS) - luvaton ilmitulo aiheuttaisi Natolle poikkeuksellisen vakavaa vahinkoa; NATO SECRET (NS) - luvaton ilmitulo aiheuttaisi Natolle vakavaa vahinkoa; NATO CONFIDENTIAL (NC) - luvaton ilmitulo aiheuttaisi Natolle vahinkoa; ja NATO RESTRICTED (NR) - luvaton ilmitulo haittaisi Naton etuja tai sen toiminnan tehokkuutta.

Liitteessä määritellään myös erityisluokkien ”ATOMAL”, ”SIOP”, ”CRYPTO” ja ”BOHEMIA” merkintöjen suojaamisessa sovellettavat sopimukset ja säännöstöt.

Luokkiin COSMIC TOP SECRET, NATO SECRET ja ATOMAL luokiteltu tieto on liitteen E mukaan tilivelvollisuuden alaista tietoa. Käytössä on oltava rekisterijärjestelmä, joka vastaa tilivelvollisuuden alaisen tiedon vastaanottamisesta, kirjaamisesta, käsittelystä, jakelusta ja hävittämisestä. Turvallisuusluokkiin NATO CONFIDENTIAL ja NATO RESTRICTED luokiteltua tietoa ei tarvitse kirjata rekisterijärjestelmään, jolleivat kansalliset säädökset ja määräykset tätä edellytä. Niiden organisaatioiden, jotka käsittelevät turvallisuusluokkaan COSMIC TOP SECRET luokiteltua tietoa, on nimettävä COSMIC-tiedon valvoja.

Liitteessä määritellään tietoturvapoikkeama, tietoturvaloukkaus, tiedon vaarantuminen ja vähäinen tietoturvapoikkeama. Kaikista tosiasiallisista ja mahdollisista tietoturvaloukkauksista on ilmoitettava viipymättä toimivaltaiselle turvallisuusviranomaiselle. Kansallinen turvallisuusviranomainen tai määrätty turvallisuusviranomainen tai Naton sotilas- tai siviilielimen johtaja välittää ilmoitukset vahingon arvioinnista ja vähentämistoimista Naton turvallisuustoimistolle. NOS voi pyytää toimivaltaisia viranomaisia tutkimaan asiaa tarkemmin ja ilmoittamaan havainnoistaan Naton turvallisuustoimistolle. NOS voi ilmoittaa asiasta myös Naton turvallisuuskomitealle.

Liite F – Viestintä- ja tietojärjestelmien turvallisuus

Liitteessä F esitetään periaatteet ja vähimmäisvaatimukset, jotka koskevat Naton turvallisuusluokitellun tiedon sekä sitä tukevien järjestelmäpalvelujen ja resurssien suojaamista viestinnässä, tallennettaessa tätä tietoa tietojärjestelmiin ja muihin sähköisin järjestelmiin sekä käsiteltäessä ja siirrettäessä sitä näissä järjestelmissä (viestintä- ja tietojärjestelmien turvallisuus). Liitteessä kuvataan tiedon luottamuksellisuutta, eheyttä, käytettävyyttä, aitoutta ja kiistämättömyyttä koskevat turvallisuustavoitteet. Kun yritykset käsittelevät turvallisuusluokiteltua tietoa sopimusten perusteella, sovelletaan lisäksi erityisiä yritysturvallisuustoimia (ks. liite G).

Kaikkien Naton turvallisuusluokiteltua tietoa käsittelevien kansallisten viestintä- ja tietojärjestelmien on läpäistävä turvallisuusakkreditointi, jossa osoitetaan turvallisuustavoitteiden toteutuminen. Turvallisuusakkreditoinnilla todetaan, että asianmukainen suojauksen taso on saavutettu ja sitä ylläpidetään.

Liitteessä F luetellaan asianmukaiset turvallisuustoimenpiteet, joita on sovellettava kaikkiin Naton turvallisuusluokiteltua tietoa käsitteleviin viestintä- ja tietojärjestelmiin, jotta saavutetaan tiedon ja sitä tukevien järjestelmäpalvelujen ja resurssien suojaamisen turvallisuutavoitteet. Naton tietoliikenne- ja tietojärjestelmien turvallisuusriskien hallinnalla varmistetaan järjestelmän haavoittuvuuksien ja turvallisuusvaatimusten mukaisuuden jatkuva arviointi.

Kun Naton turvallisuusluokiteltua tietoa siirretään sähköisesti, on toteutettava erityiset toimenpiteet turvallisuustavoitteiden saavuttamiseksi näissä siirroissa. Turvallisuusluokkaan NATO SECRET ja sitä ylempiin luokkiin luokitellun tiedon luottamuksellisuus on tietoa siirrettäessä suojattava Naton sotilaskomitean hyväksymillä salaustuotteilla ja –menetelmillä. Turvallisuusluokkaan NATO CONFIDENTIAL tai NATO RESTRICTED luokitellun tiedon luottamuksellisuus on tietoa siirrettäessä suojattava joko Naton sotilaskomitean tai Naton jäsenvaltion hyväksymillä salaustuotteilla tai –menetelmillä.

Liitteessä kuvataan kansallisen viestintä- ja tietojärjestelmien turvallisuusviranomaisen (NCSA), Naton salausaineiston hallinnasta vastaavan kansallisen jakeluviranomaisen sekä akkreditointiviranomaisten tehtävät.

Liite G – Turvallisuusluokiteltujen hankkeiden turvallisuus ja yritysturvallisuus

Liitteessä G kuvataan Naton turvallisuusluokitellun tiedon turvallisuutta yrityksissä koskevat periaatteet ja vähimmäisvaatimukset. Yritysturvallisuus on suojaustoimien ja –menettelyjen soveltamista sellaisen turvallisuusluokitellun tiedon katoamisen tai vaarantumisen estämiseksi, havaitsemiseksi ja korjaamiseksi, jota yritykset käsittelevät hankesopimusten perusteella. Yrityksille annettava ja yritysten kanssa tehtävien hankesopimusten perusteella tuotettava Naton turvallisuusluokiteltu tieto sekä yritysten kanssa tehtävät hankesopimukset on suojattava Naton turvallisuusperiaatteiden ja niitä tukevien ohjeiden mukaisesti. Hankeosapuolen ja alihankkijoiden edellytetään sitoutuvan kaikkiin kansallisten turvallisuusviranomaisten tai määrättyjen turvallisuusviranomaisten määräämiin toimiin hankeosapuolen tuottaman tai Naton turvallisuusluokitellun tiedon suojaamiseksi. Liite sisältää erilliset määräykset Naton ulkopuolisten valtioiden hankeosapuolten kanssa tehtävistä hankesopimuksista.

Kunkin Naton jäsenvaltion kansallisen turvallisuusviranomaisen tai määrätyn turvallisuusviranomaisen vastuulla on varmistaa, että sen toimivaltaan kuuluvat yhteisöt, jotka tarvitsevat pääsyn turvallisuusluokkaan NATO CONFIDENTIAL ja sitä ylempiin luokkiin luokiteltuun tietoon, ovat toteuttaneet tarvittavat suojaustoimet saadakseen todistuksen yritysturvallisuusselvityksestä (Facility Security Clearance, FSC). Yritysten työntekijöillä, jotka tarvitsevat pääsyn turvallisuusluokkaan NATO CONFIDENTIAL ja sitä ylempiin turvallisuusluokkiin luokiteltuun Naton tietoon, on oltava asianmukainen todistus henkilöturvallisuusselvityksestä.

Liite G sisältää myös kansainvälisiin vierailuihin liittyviä valvontamenettelyitä koskevat periaatteet sekä Naton hankkeeseen tai ohjelmaan lainattavaa henkilöstöä sekä Naton turvallisuusluokitellun aineiston kansainvälisiin siirtoihin ja kuljettamiseen sovellettavat turvallisuusperiaatteet.

Liite H – Turvallisuus suhteissa Naton ulkopuolisiin toimijoihin

Turvallisuusääntöjen liitteessä H kuvataan ne periaatteet ja vähimmäisvaatimukset, joita on noudatettava suojattaessa Naton ulkopuolisille valtioille ja muille Naton ulkopuolisille elimille (esim. kansainvälisille järjestöille) luovutettavaa tai näiden pääsyoikeuden piiriin kuuluvaa Naton turvallisuusluokiteltua tietoa. Lisätietoja ja vaatimuksia Naton ulkopuolisille toimijoille luovutettavan tai näiden pääsyoikeuden piiriin kuuluvan Naton turvallisuusluokitellun tiedon suojaamiseksi on Naton turvallisuusperiaatteita tukevassa ohjeessa turvallisuudesta Naton suhteissa Naton ulkopuolisiin toimijoihin.

Naton turvallisuusluokitellun tiedon jakamisen Naton ulkopuolisten toimijoiden kanssa tulee lähtökohtaisesti tapahtua Pohjois-Atlantin neuvoston hyväksymän Naton yhteistyötoiminnan yhteydessä, mutta poikkeustapauksissa se voi tapahtua myös tällaisen toiminnan ulkopuolella.

Ennen Naton turvallisuusluokitellun tiedon jakamista Naton ulkopuolisen toimijan kanssa kyseisen toimijan ja Naton on tullut tehdä turvallisuussopimus. Turvallisuussopimuksen turvallisuusperiaatteita tuetaan asianmukaisella hallinnollisten järjestelyjen kokonaisuudella. Mikäli turvallisuussopimusta ei ole tehty, ja tietoa on kuitenkin välttämätöntä jakaa oikea-aikaisesti, on tullut antaa turvallisuusvakuutus.

Erityiset määräykset koskien Naton ulkopuolisille toimijoille luovutettavan tai näiden pääsyoikeuden piiriin kuuluvan Naton turvallisuusluokitellun tiedon suojaamisesta koskevat henkilöstöturvallisuutta, toimitilaturvallisuutta, tietoaineistoturvallisuutta, luovuttajaviranomaisia, luovutettua tietoa koskevaa kirjanpitoa sekä viestintä- ja tietojärjestelmien turvallisuutta. Liitteessä H esitetään myös tietoturvapoikkeamien käsittelyä koskevat vaatimukset.

Sanasto

Turvallisuussääntöjen liitteenä on myös sanasto, joka sisältää säännöissä käytettyjen keskeisten termien määritelmät.

Keskeisimmät muutokset nykytilaan

Suomi noudattaa jo tällä hetkellä Naton turvallisuussääntöjä C-M(2002)49-REV1 vuonna 2012 tehdyn hallinnollisen järjestelyn nojalla. Naton turvallisuussopimukseen sitoutuminen ei siten muuta nykytilannetta merkittävästi. Tällä hetkellä Suomen viranomaisten tulkinnan apuna on tulkintaohje AC/35-D/1038, “Supporting Document on the Security Protection of NATO Information Released to Non-NATO Nations and International Organisations”, joka on tarkoitettu Natoon kuulumattomien maiden turvallisuusviranomaisten käyttöön. Naton turvallisuusluokitellun tiedon luovuttaminen Suomelle Natoon kuulumattomana maana on edellyttänyt aikanaan erityistä Naton turvallisuustoimiston turvallisuussopimuksen täytäntöönpanon sertifiointiprosessin kautta antamaa muodollista vakuutusta siitä, että tietoa suojataan Suomessa Naton turvallisuussäännöstön minimistandardien mukaisesti.

Rauhankumppanina Nato-asiakirjojen saaminen on perustunut aina tiedon alkuperäisen luovuttajan kirjalliseen suostumukseen tai NAC:in hyväksymään yhteistyöhön taikka Naton toimintaan, johon Suomi osallistuu NAC:n tuella. Erona nykytilanteeseen on myös se, että Naton jäsenenä Suomi voi saada korkeimman turvallisuusluokan COSMIC TOP SECRET –tason asiakirjoja, joita ei pääsääntöisesti luovuteta Natoon kuulumattomille maille. Joiltakin osin turvallisuusluokiteltujen tietojen käsittelyvaatimukset ovat Nato-jäsenten kohdalla joustavammat. Esimerkiksi NATO CONFIDENTIAL- ja NATO RESTRICTED –asiakirjojen rekisteröinti jätetään kansallisen lainsäädännön varaan. Nato-jäsenyyden myötä Naton turvallisuustoimisto te-

kee Suomeen määräajoin Naton turvallisuusluokitellun tiedon suojaamiseen tarkoitettujen turvallisuusjärjestelyjen *tarkastuksia.* Rauhankumppanuuden aikana Naton turvallisuustoimisto on tehnyt Suomeen niin sanottuja *tarkastusvierailuja*.

Naton turvallisuusluokitellun tiedon suojaamiseen tulee käyttää hyväksyttyjä salaustuotteita. Luokkien NATO SECRET ja COSMIC TOP SECRET tiedon suojaaminen edellyttää Naton sotilaskomitean (NAMILCOM, NATO Military Committee) hyväksymän salaustuotteen käyttöä. Luokkien NATO CONFIDENTIAL ja NATO RESTRICTED tiedon suojaamiseen voidaan käyttää myös jäsenmaan NCSA-viranomaisen hyväksymiä kansallisia salaustuotteita. Jäsenyyden myötä Liikenne- ja viestintävirasto voi arvioida ja hyväksyä kansallisia salaustuotteita NC- ja NR-luokkien tietojen suojaamiseen.

9 Suomen ja Pohjois-Atlantin liiton kesken vaihdettavan turvallisuusluokitellun tiedon suojaamiseksi tehty hallinnollinen järjestely ja Pohjois-Atlantin liiton kanssa tehty tietoturvallisuussopimus

Pohjois-Atlantin liiton kanssa vuonna 1994 tehdyllä sopimuksella Suomi sitoutui luokittelemaan ja suojaamaan rauhankumppanuusohjelman puitteissa Natolta saadun aineiston sekä laatimaan turvallisuusselvitykset niistä henkilöistä, joilla on pääsy suojattuun aineistoon. Sopimuksen liitteenä on selvitys Naton käyttämästä asiakirjojen turvallisuusluokittelusta sekä tiettyjen hallinnollisten kysymysten järjestämisestä sopimuksen toimeenpanemiseksi.

Vuonna 2012 Suomi teki Pohjois-Atlantin liiton kanssa sopimusta täydentävän hallinnollisen järjestelyn turvallisuusluokitellun tiedon suojaamiseksi. Järjestelyssä määrätään turvallisuusviranomaisista, sovellettavista määritelmistä, turvallisuusluokitellun tiedon merkitsemisestä, suojaamisesta ja käytöstä, pääsystä turvallisuusluokiteltuun tietoon, turvallisuusluokitellun tiedon lähettämisestä, immateriaalioikeuksista, turvallisuusvaatimusten yksityiskohdista, järjestelyn noudattamisesta ja turvallisuustarkastuksista, vierailuista, tarkastusvierailuista, tiedon katoamisesta ja vaarantumisesta, kustannuksista, riitojen ratkaisusta sekä tavanomaisista loppumääräyksistä.

Suomen liittyessä Natoon sen tulee liittyä myös vuonna 1997 Pohjois-Atlantin sopimuksen osapuolten välillä tietoturvallisuudesta tehtyyn sopimukseen, jonka määräykset korvaavat vuonna 1994 tehdyn sopimuksen ja vuonna 2012 tehdyn järjestelyn. Sopimus ja järjestely eivät sisällä määräystä niiden irtisanomisesta, mutta Naton kanssa on käyty keskusteluja sopimuksen ja järjestelyn päättämisestä valtiosopimusoikeutta koskevan Wienin yleissopimuksen (SopS 32 ja 33/1980) 54 artiklan b kohdan mukaisesti. Näin ollen sopimus ja järjestely on tarkoitus irtisanoa ja niiden voimaansaattamislaki on tarpeen kumota. Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 15 §:n mukaan lain tietoturvallisuustoimenpiteitä koskevia säännöksiä sovelletaan niin kauan kuin se turvallisuusluokituksen perusteena olevan yleisen edun vuoksi on tarpeen silloinkin, kun sopimus tai säädös, johon säännösten soveltaminen perustuu, ei enää ole voimassa.

10 Lakiehdotusten säännöskohtaiset perustelut

10.1 Laki tietoturvallisuudesta Pohjois-Atlantin sopimuksen osapuolten välillä tehdystä sopimuksesta ja turvallisuussäännöistä

1 §. Pykälä sisältäisi tavanomaisen blankettilain säännöksen siitä, että sopimuksen ja sen nojalla annettujen turvallisuussääntöjen, sellaisina kuin ne ovat muutettuina 20.11.2020 annetussa asiakirjassa C-M(2002)49-REV-1, lainsäädännön alaan kuuluvat määräykset ovat lakina voimassa sellaisina kuin Suomi on niihin sitoutunut. Sopimuksen ja turvallisuussääntöjen lainsäädännön

alaan kuuluvia määräyksiä käsitellään tarkemmin eduskunnan suostumuksen tarpeellisuutta käsittelevässä jaksossa.

2 §. Pykälä sisältäisi tavanomaisen blankettilain säännöksen, joka koskee sopimuksen ja turvallisuussääntöjen muiden kuin lainsäädännön alaan kuuluvien määräysten voimaansaattamista valtioneuvoston asetuksella.

3 §. Pykälä sisältäisi tavanomaisen blankettilain säännöksen, jonka mukaan lain voimaantulosta säädetään valtioneuvoston asetuksella. Voimaantulosta säätäminen asetuksella on tarpeen, jotta lain voimaantulo tapahtuu samanaikaisesti, kun sopimuksen voimaantulo Suomen osalta.

10.2 Laki Suomen ja Pohjois-Atlantin liiton kesken vaihdettavan turvallisuusluokitellun tiedon suojaamiseksi tehdyn hallinnollisen järjestelyn ja Pohjois-Atlantin liiton kanssa tehdyn tietoturvallisuussopimuksen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta annetun lain kumoamisesta

1 §. Lakiehdotuksen 1 §:n nojalla Suomen ja Pohjois-Atlantin liiton kesken vaihdettavan turvallisuusluokitellun tiedon suojaamiseksi tehdyn hallinnollisen järjestelyn ja Pohjois-Atlantin liiton kanssa tehdyn tietoturvallisuussopimuksen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta annettu laki (945/2012) kumottaisiin.

2 §. Lain voimaantulosta säädettäisiin valtioneuvoston asetuksella. Laki on tarkoitus saattaa voimaan samanaikaisesti sopimusten irtisanomisen voimaantulon kanssa.

11 Voimaantulo

Tietoturvallisuudesta Pohjois-Atlantin sopimuksen osapuolten välillä tehty sopimus tulee Suomen osalta voimaan kolmenkymmenen päivän kuluttua siitä päivästä, kun Suomi tallettaa tietoturvallisuussopimusta koskevan liittymiskirjansa Amerikan yhdysvaltojen hallituksen huostaan. Ehdotetaan, että esitykseen sisältyvä sopimuksen voimaansaattamislaki tulee voimaan valtioneuvoston asetuksella säädettävänä ajankohtana samanaikaisesti, kun sopimus tulee Suomen osalta voimaan.

Tarkoituksena on, että Suomen ja Pohjois-Atlantin liiton kesken vaihdettavan turvallisuusluokitellun tiedon suojaamiseksi tehdyn hallinnollisen järjestelyn ja Pohjois-Atlantin liiton kanssa tehdyn tietoturvallisuussopimuksen irtisanominen tulee voimaan samaan aikaan, kun Suomen liittyminen Pohjois-Atlantin sopimuksen osapuolten välillä tietoturvallisuudesta tehtyyn sopimukseen tulee voimaan. Ehdotetaan, että esitykseen sisältyvä laki kyseisten sopimusten lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta annetun lain kumoamisesta tulee voimaan valtioneuvoston asetuksella säädettävänä ajankohtana samanaikaisesti, kun irtisanominen tulee voimaan.

12 Ahvenanmaan maakuntapäivien suostumus

Ahvenanmaan itsehallintolain (1144/1991) 59 §:n 1 momentin mukaan, jos valtiosopimus tai muu kansainvälinen velvoite, johon Suomi sitoutuu, sisältää määräyksen itsehallintolain mukaan maakunnan toimivaltaan kuuluvassa asiassa, maakuntapäivien on, jotta määräys tulisi voimaan maakunnassa, hyväksyttävä säädös, jolla määräys saatetaan voimaan.

Tietoturvallisuudesta Pohjois-Atlantin sopimuksen osapuolten välillä tehty sopimus ei sisällä Ahvenanmaan maakunnan toimivaltaan kuuluvia määräyksiä, eikä siten edellytä maakunnan suostumusta Ahvenanmaan itsehallintolain 59 §:n mukaisesti.

Itsehallintolain perusteella maakuntapäivien hyväksyminen ei ole tarpeen sopimuksen irtisanomiselle tai sopimuksen voimaansaattamislain kumoamista koskevalle laille.

13 Suhde muihin esityksiin

Tämä hallituksen esitys liittyy 5.12.2022 annettuun hallituksen esitykseen eduskunnalle Pohjois-Atlantin sopimuksen sekä Pohjois-Atlantin liiton, kansallisten edustajien ja kansainvälisen henkilöstön asemasta tehdyn sopimuksen hyväksymiseksi ja voimaansaattamiseksi (HE 315/2022 vp). Suomi on liittymisneuvotteluissa sitoutunut liittymään Naton tietoturvallisuussopimukseen 12 kuukauden kuluessa siitä, kun Suomi on tallettanut Pohjois-Atlantin sopimusta koskevan liittymiskirjansa.

Tietoturvallisuutta koskevia määräyksiä sisältyy myös Naton sopimukseen puolustukseen liittyvien, patentoitavaksi haettujen keksintöjen salassapidon vastavuoroiseksi turvaamiseksi, Naton sopimukseen teknisten tietojen välittämisestä puolustustarkoituksiin sekä Pohjois-Atlantin sopimuksen osapuolten väliseen sopimukseen ydinpuolustustietoja koskevasta yhteistyöstä. Sopimusten hyväksymisestä annetaan erilliset hallituksen esitykset.

Erillinen hallituksen esitys annetaan myös Pohjois-Atlantin sopimuksen sopimuspuolten välillä niiden joukkojen asemasta tehdyn sopimuksen (Nato SOFA) sekä Pohjois-Atlantin sopimuksen mukaisesti perustettujen kansainvälisten sotilasesikuntien asemasta tehdyn pöytäkirjan (Pariisin pöytäkirja) hyväksymiseksi.

14 Eduskunnan suostumuksen tarpeellisuus ja käsittelyjärjestys

14.1 Eduskunnan suostumuksen tarpeellisuus

Sopimus tietoturvallisuudesta Pohjois-Atlantin sopimuksen osapuolten välillä

Perustuslain 94 §:n 1 momentin mukaan eduskunta hyväksyy sellaiset valtiosopimukset ja muut kansainväliset velvoitteet, jotka sisältävät lainsäädännön alaan kuuluvia määräyksiä tai ovat muutoin merkitykseltään huomattavia taikka vaativat perustuslain mukaan muusta syystä eduskunnan hyväksymisen. Eduskunnan hyväksyminen vaaditaan myös tällaisen velvoitteen irtisanomiseen. 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 (PeVL 11/2000 vp ja PeVL 12/2000 vp).

Sopimuksen 1 artiklan i kohdassa yhdessä sopimuksen I ja II liitteen kanssa määritellään, mitä tarkoitetaan suojattavalla turvallisuusluokitellulla tiedolla. Koska määritelmä vaikuttaa joko suoraan tai välillisesti sopimuksen lainsäädännön alaan kuuluvien aineellisten määräysten tulkintaan ja soveltamiseen, 1 artiklan i kohta ja I ja II liite edellyttävät eduskunnan hyväksymistä (PeVL 6/2001 vp).

Sopimuksen 1 artiklan ii ja ii kohdassa määrätään sopimuksen soveltamisalaan piiriin kuuluvan turvallisuusluokitellun tiedon suojaamiseksi tarvittavista toimenpiteistä, jotka rajoittavat turval-

lisuusluokitellun tiedon luovuttamista sekä sen käyttöä. Artiklassa on kyse sopimuksen keskeisestä määräyksestä, jonka perusteella Suomi voi suojata sopimuksessa tarkoitettua turvallisuusluokiteltua tietoa ilman julkisuuslaissa säädettyä vahinkoedellytysarviointia. Määräys kuuluu lainsäädännön alaan.

Sopimuksen 2 artiklan mukaan osapuolet varmistavat kansallisen turvallisuusviranomaisen perustamisen Naton toimintaa varten toteuttamaan suojaavia turvatoimia. Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 4 §:ssä on säännökset Suomen kansallisesta turvallisuusviranomaisesta ja määrätyistä turvallisuusviranomaisista sekä heidän toimivaltuuksistaan. Artiklan velvoite kansallisesta turvallisuusviranomaisesta kuuluu lainsäädännön alaan.

Sopimuksen 2 artiklan mukaan osapuolet laativat ja panevat täytäntöön turvallisuusvaatimuksia, joilla varmistetaan turvallisuusluokitellun tiedon yhteinen suojauksen taso. Artikla sisältää oikeusperustan Naton turvallisuusluokitellun tiedon suojaamista koskeville säännöille ja direktiiveille, joita Suomi Natoon liityttyään sitoutuu noudattamaan. Artiklassa delegoidaan turvallisuusvaatimuksia koskevaa sopimuksentekotoimivaltaa Pohjois-Atlantin neuvostolle. Delegointia koskeva määräys kuuluu lainsäädännön alaan.

Sopimuksen 3 artiklassa määrätään osapuolten velvollisuudesta tehdä asianmukaisesti turvallisuusselvitys henkilöistä, jotka virallisia tehtäviään hoitaessaan tarvitsevat tai saattavat saada turvallisuusluokkaan CONFIDENTIAL ja sitä ylempiin turvallisuusluokkiin kuuluvaa tietoa. Artikla sisältää turvallisuusselvitysmenettelyjen jäännösriskiä ja osapuolten yhteistyötä koskevat määräykset. Suomessa turvallisuusselvityksen kohteena olevista henkilöistä sekä selvityksessä sovellettavasta menettelystä säädetään turvallisuusselvityslaissa. Sopimuksen 3 artikla sisältää lainsäädännön alaan kuuluvia määräyksiä.

Naton turvallisuussäännöt

Naton turvallisuussäännöstön keskeisimmät turvallisuuden periaatteet ja vähimmäisvaatimukset sisältyvät Pohjois-Atlantin neuvoston (NAC) hyväksymiin Naton turvallisuussääntöihin C-M(2002)49-REV1. Kansainvälisten tietoturvallisuussopimusten nojalla hyväksyttyjä turvallisuussäännöstöjä ei ole tapana saattaa kansallisesti voimaan. Naton turvallisuussäännöt sisältävät kuitenkin seuraavassa lueteltuja lainsäädännön alaan kuuluvia määräyksiä, jotka eivät ilmene suoraan tietoturvallisuussopimuksen tekstistä. Sellaisille määräyksille katsotaan tarpeelliseksi pyytää eduskunnan hyväksyminen ja saattaa ne kansallisesti voimaan (PeVL 19/2010 vp, s. 5-6). Turvallisuussääntöjen teksti on hallituksen esityksen liitteenä.

Turvallisuussääntöjen liite A sisältää varsinaisen tietoturvallisuussopimuksen tekstin, jonka lainsäädännön alaan kuuluvia määräyksiä on selostettu edellä.

Turvallisuussääntöjen B liitteen 1(b) kohta sisältää perusperiaatteen tarpeesta tietoon (need-to-know). Asiasta säädetään kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 6 §:n 3 momentissa. Liitteen 3 kohdassa määritellään kansallisen turvallisuusviranomaisen tehtävät ja 5 kohdassa edellytetään, että Naton jäsenvaltiolla on määrätty turvallisuusviranomainen yhteisöturvallisuusmääräysten täytäntöön panemiseksi. Suomen turvallisuusviranomaisista ja niiden tehtävistä säädetään kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 4 §:ssä. Liitteen 9(f) kohdassa annetaan Naton turvallisuustoimiston tehtäväksi suorittaa myös jäsenvaltioissa säännöllisiä turvallisuustarkastuksia Naton turvallisuusluokitellun tiedon suojaamiseksi. Kansainvälisen toimielimen vierailuista turvallisuustarkastusten suorittamiseksi säädetään kansainvälisistä turvallisuusvelvoitteista annetun lain 18 §:ssä.

Turvallisuussääntöjen C liitteen 7 kohdassa määritellään korkeassa valtion tehtävässä olevat henkilöt, esimerkiksi valtion ja hallitusten päämiehet, ministerit sekä parlamentin ja tuomioistuinlaitoksen jäsenet, joiden osalta tarve henkilöturvallisuusselvitykseen määräytyy kansallisen lainsäädännön ja säännösten mukaisesti. Myös näillä henkilöryhmillä tulee olla tarve tietoon ja heille tulee selvittää turvallisuusvelvoitteet.

Turvallisuussääntöjen E liitteen 6 kohdassa määritellään Naton turvallisuusluokat ja niiden merkitseminen. Liitteen 32-39 kohdassa määritellään tietoturvapoikkeama, tietoturvaloukkaus, tiedon vaarantuminen ja vähäinen tietoturvapoikkeama ja niitä koskevat selvitys- ja raportointivelvollisuudet. Rikkomusten selvittämisestä ja niistä ilmoittamisesta säädetään kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 19 §:ssä.

Turvallisuussääntöjen F liite sisältää tietoaineistoturvallisuutta koskevat määräykset. Turvallisuussääntöjen F liitteen 3 kohta koskee tietojärjestelmien akkreditointivelvoitetta. Tietojärjestelmien arvioinnista säädetään laissa viranomaisten tietojärjestelmien arvioinnista. Lain 8 §:n mukaan valtioneuvoston asetuksella voidaan säätää, että 8 §:ssä tarkoitettu todistus on hankittava sellaisen valtionhallinnon viranomaisen määräysvallassa olevasta tietojärjestelmästä tai tietoliikennejärjestelystä, jossa käsitellään turvallisuusluokkaan I tai II kuuluviksi luokiteltuja asiakirjoja. Liitteen 13.4 koskee NCSA:n tehtäviä. Suomen turvallisuusviranomaisista ja niiden tehtävistä säädetään kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 4 §:ssä, jonka mukaan Liikenne- ja viestintävirasto toimii NSA:n asiantuntijana tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuutta koskevissa asioissa.

Turvallisuussääntöjen G liitteen 4 kohta sisältää vaatimuksen yritysturvallisuusselvitystodistuksesta, kun yritys käsittelee turvallisuusluokkaan CONFIDENTIAL tai sitä ylempiin turvallisuusluokkiin kuuluvaa tietoa. Liitteen 10 kohta sisältää yritykselle asetettavan sopimusvelvoitteen luokitellun tiedon suojaamisesta. Yritysturvallisuusselvityksistä säädetään turvallisuusselvityslain 5 luvussa ja kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 12 §:ssä.

14.2 Käsittelyjärjestys

Tietoturvallisuudesta Pohjois-Atlantin liiton osapuolten välillä tehdyssä sopimuksessa määritellään Naton tietoturvallisuutta koskevat säännöt, joiden mukaan Naton jäsenmaiden tulee käsitellä turvallisuusluokiteltua tietoa. Kyse olisi erityissääntelystä suhteessa kansallisten viranomaisten asiakirjojen julkisuutta koskevaan yleislainsäädäntöön. Perustuslain 12 §:n mukaan viranomaisen asiakirjat ovat julkisia, jollei niiden julkisuutta ole välttämättömien syiden vuoksi lailla erikseen rajoitettu. Tietoturvallisuussopimus sisältää tällaisia perustuslain 12 §:n tarkoittamia sääntöjä, joilla julkisuutta rajoitetaan välttämättömien syiden vuoksi.

Kansainväliset tietoturvallisuussopimukset ovat vakiintunut tapa säännellä turvaluokiteltujen tietojen vaihtoa Suomen ja jonkin toisen valtion tai kansainvälisen järjestön välillä. Suomella on tällä hetkellä voimassa yhteensä 26 tietoturvallisuussopimusta, jotka eduskunta on hyväksynyt yksinkertaisella äänten enemmistöllä ja käsitellyt niiden voimaansaattamislait tavallisen lain säätämisjärjestyksessä. Perustuslakivaliokunta on katsonut lausunnossaan PeVL 39/1997 vp käsitellessään Suomen ja Länsi-Euroopan unionin (WEU) välistä tietoturvallisuussopimusta (ei enää voimassa), että julkisuusperiaatteen rajoittamista sopimuksen ja voimaansaattamislain 2 §:n mukaisesti voitiin pitää välttämättömänä Suomen ja WEUn yhteistyön mahdollistamisen kannalta. Salassapitointressi vastasi myös niitä perusteita, jotka mainittiin tuolloin voimassa olleen yleisten asiakirjain julkisuudesta annetun lain (83/1951) 9 §:ssä. Sopimuksen voimaansaattamislaki voitiin käsitellä tavallisen lain säätämisjärjestyksessä. Sen jälkeen on säädetty niin ikään tavallisen lain säätämisjärjestyksessä laki kansainvälisistä tietoturvallisuusvelvoitteista,

jossa säädetään viranomaisten toimenpiteistä kansainvälisten tietoturvallisuusvelvoitteiden toteuttamiseksi.

Suomen ja Naton välillä vuonna 2012 tehty hallinnollinen järjestely turvallisuusluokitellun tiedon suojaamisesta on hyväksytty yksinkertaisella äänten enemmistöllä ja sen voimaansaattamislaki on säädetty tavallisen lain säätämisjärjestyksessä. Samassa yhteydessä saatettiin voimaan tavallisen lain säätämisjärjestyksessä vuonna 1994 Suomen ja Naton välillä tehdyn sopimuksen lainsäädännön alaan kuuluvat määräykset. Hallituksen esityksen mukaan eduskunnan hyväksyttävänä olleen hallinnollisen järjestelyn 5 artiklan määräykset eivät laajentaneet salassapitovelvollisuutta siitä, mitä salassapidosta on säädetty kansainvälisistä tietoturvallisuusvelvoitteista annetun 6 §:ssä (HE 139/2012 vp).

Nyt käsiteltävänä olevalla tietoturvallisuussopimuksella sitoudutaan noudattamaan vastaavia tietoturvallisuusvelvoitteita, joihin Suomi on jo vuonna 1994 tehdyllä tietoturvallisuussopimuksella ja 2012 tehdyllä hallinnollisella järjestelyllä sitoutunut. Tietoturvallisuussopimuksen velvoitteiden voidaan katsoa olevan välttämättömiä rajoituksia julkisuudesta Pohjois-Atlantin sopimuksessa tarkoitetun yhteistyön mahdollistamiseksi.

Nyt hyväksyttävänä olevan sopimuksen 2 artiklan mukaan osapuolet laativat ja panevat täytäntöön turvallisuusvaatimuksia, joilla varmistetaan turvallisuusluokitellun tiedon yhteinen suojauksen taso. Edellä jaksossa 8.2. kuvataan näitä tietoturvallisuussopimuksen täytäntöönpanoa koskevia määräyksiä. Turvallisuussäännöstössä on oikeudellisesti kyse tietoturvasopimuksen toteutumista turvaavista teknisistä määräyksistä.

Suomen perustuslakia on muutettu vuonna 2012 siten, että perustuslain 94 §:n 2 momentin ja 95 §:n 2 momentin säännösten mukaan Suomen täysivaltaisuuden kannalta *merkittävän* toimivallan siirrosta Euroopan unionille, kansainväliselle järjestölle tai kansainväliselle toimielimelle päätetään kahden kolmasosan enemmistöllä. Sen sijaan tavallisella äänestenemmistöllä voidaan päättää muuta kuin merkittävää toimivallan siirtoa koskevien kansainvälisten velvoitteiden hyväksymisestä ja voimaansaattamisesta.

Perustuslain muuttamista koskevassa hallituksen esityksessä todetaan, että eduskunnan toimivallan siirroissa on tavanomaisesti kyse sellaisista kansainvälisistä sopimusjärjestelyistä, joissa siirretään vähäisessä määrin säädösvaltaa kansainväliselle toimielimelle varsin teknisluonteisessa sääntelyssä tai hyvin rajatuilla aloilla, ja että tällaisen toimivallan siirtämisestä voitaisiin vastaisuudessa päättää tavallisella enemmistöllä (HE 60/2010 vp, s.28).

Sopimuksen 2 artiklassa delegoidaan turvallisuusvaatimuksia koskevaa sopimuksentekotoimivaltaa Pohjois-Atlantin neuvostolle. Kyseessä ei olisi kuitenkaan perustuslain täysivaltaisuussääntelyn kannalta merkittävä sopimuksentekovallan delegointi vaan nykyaikaisessa kansainvälisessä yhteistoiminnassa tavanomainen sopimuksen täytäntöönpanon tarkempi sääntely, josta Pohjois-Atlantin sopimuksen osapuolet päättävät yksimielisesti. Tietoturvallisuutta koskevia määräyksiä sovelletaan pääosin viranomaisissa. Yrityksille niillä on merkitystä silloin, jos ne osallistuvat turvallisuusluokiteltuun sopimukseen, joka sisältää Naton turvallisuusluokitellun tiedon käsittelyä. Yksityisille ihmisille sopimuksella ja tietoturvallisuussäännöstöllä on lähinnä välillistä merkitystä.

Perustuslakivaliokunta on katsonut, että lainsäädännön alaan kuuluvien teknisluonteisten täytäntöönpanomääräysten antaminen ei ole ollut ongelmallista, mutta siltä osin, kun ne ovat kuuluneet lainsäädännön alaan, on valiokunta edellyttänyt pääsääntöisesti niiden voimaan saattamista ja julkaisemista (PeVL 19/2010 vp, s. 5 ja 6). Asiakirjaan C-M(2002)49-REV1 sisältyvät Naton turvallisuussäännöt sisältävät joitakin, edellä jaksossa 14.1. kuvattuja lainsäädännön

alaan kuuluvia määräyksiä, jotka eivät ilmene suoraan tietoturvallisuussopimuksen tekstistä. Sellaisille määräyksille pyydetään eduskunnan hyväksyminen, ne on sisällytetty sopimuksen voimaansaattamislakiin ja turvallisuussäännöt julkaistaan yhdessä Naton turvallisuussopimuksen kanssa Suomen säädöskokoelman sopimussarjassa. Jatkossa turvallisuussääntöjen muutoksista julkaistaisiin sopimussarjassa Suomen säädöskokoelmasta annetun lain (188/2000) 9 §:n 2 momentin mukainen ilmoitus.

Koska tietoturvallisuudesta Pohjois-Atlantin liiton osapuolten välillä tehty sopimus ja turvallisuussäännöt eivät sisällä määräyksiä, jotka koskisivat perustuslakia sen 94 §:n 2 momentissa tai 95 §:n 2 momentissa tarkoitetulla tavalla, sopimus ja turvallisuussäännöt voidaan hallituksen käsityksen mukaan hyväksyä äänten enemmistöllä ja ehdotus niiden voimaansaattamislaiksi tavallisen lain säätämisjärjestyksessä.

Perustuslakivaliokunnan ja ulkoasianvaliokunnan kannan mukaan kansainvälisen velvoitteen irtisanomista koskeva päätös voidaan tehdä yksinkertaisella äänten enemmistöllä (PeVM 10/1998 vp ja UaVL 6/1998 vp). Suomen ja Pohjois-Atlantin liiton kesken vaihdettavan turvallisuusluokitellun tiedon suojaamiseksi tehdyn hallinnollisen järjestelyn ja Pohjois-Atlantin liiton kanssa tehdyn tietoturvallisuussopimuksen irtisanomisen hyväksymisestä voidaan päättää äänten enemmistöllä ja laki kyseisten sopimusten lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta annetun lain kumoamisesta voidaan hyväksyä tavallisen lain säätämisjärjestyksessä.

1. ponsi

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

että eduskunta hyväksyisi tietoturvallisuudesta Pohjois-Atlantin sopimuksen osapuolten välillä Brysselissä 6.3.1997 tehdyn sopimuksen ja sen nojalla annetut turvallisuussäännöt sellaisina kuin ne ovat muutettuina 20.11.2020 hyväksytyssä asiakirjassa C-M(2002)49-REV1 ja

että eduskunta hyväksyisi Suomen ja Pohjois-Atlantin liiton kesken vaihdettavan turvallisuusluokitellun tiedon suojaamiseksi Helsingissä 3.7.2012 tehdyn hallinnollisen järjestelyn sekä Pohjois-Atlantin liiton kanssa Brysselissä 22.9.1994 tehdyn tietoturvallisuussopimuksen (SopS 7 ja 8/2013) irtisanomisen.

2. ponsi

Koska sopimukset sisältävät määräyksiä, jotka kuuluvat lainsäädännön alaan, annetaan samalla eduskunnan hyväksyttäviksi seuraavat lakiehdotukset:

1.

Laki

tietoturvallisuudesta Pohjois-Atlantin sopimuksen osapuolten välillä tehdystä sopimuksesta ja turvallisuussäännöistä

Eduskunnan päätöksen mukaisesti säädetään:

1 §

Tietoturvallisuudesta Pohjois-Atlantin sopimuksen osapuolten välillä Brysselissä 6 päivänä maaliskuuta 1997 tehdyn sopimuksen ja sen nojalla annettujen turvallisuussääntöjen, sellaisina kuin ne ovat muutettuina 20 päivänä marraskuuta 2020 hyväksytyssä asiakirjassa C-M(2002)49-REV1, lainsäädännön alaan kuuluvat määräykset ovat lakina voimassa sellaisina kuin Suomi on niihin sitoutunut.

2 §

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

3 §

Tämän lain voimaantulosta säädetään valtioneuvoston asetuksella.

2.

Laki

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

Eduskunnan päätöksen mukaisesti säädetään:

1 §

Tällä lailla kumotaan Suomen ja Pohjois-Atlantin liiton kesken vaihdettavan turvallisuusluokitellun tiedon suojaamiseksi tehdyn hallinnollisen järjestelyn ja Pohjois-Atlantin liiton kanssa tehdyn tietoturvallisuussopimuksen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta annettu laki (945/2012).

2 §

Tämän lain voimaantulosta säädetään valtioneuvoston asetuksella.

Helsingissä x.x.20xx

Pääministeri

Etunimi Sukunimi

Ulkoministeri Etunimi Sukunimi

SOPIMUS POHJOIS-ATLANTIN SOPIMUKSEN OSAPUOLTEN VÄLILLÄ TIETOTURVALLISUUDESTA

Washingtonissa 4 päivänä huhtikuuta 1949 allekirjoitetun Pohjois-Atlantin sopimuksen osapuolet, jotka

vahvistavat, että tehokas poliittinen neuvottelu, yhteistyö ja suunnittelu puolustusasioissa sopimuksen tavoitteiden saavuttamiseksi edellyttävät turvallisuusluokitellun tiedon vaihtamista osapuolten välillä,

katsovat, että Pohjois-Atlantin sopimuksen osapuolten hallitusten välillä tarvitaan määräyksiä sellaisen turvallisuusluokitellun tiedon vastavuoroisesta suojaamisesta ja turvaamisesta, jota ne voivat vaihtaa keskenään,

ymmärtävät, että turvallisuusvaatimuksille ja menettelyille tarvitaan yleiset puitteet, ja

toimivat omasta puolestaan ja Pohjois-Atlantin liiton puolesta,

ovat sopineet seuraavasta:

1 artikla

Osapuolet

i. suojaavat ja turvaavat

a. turvallisuusluokitelluksi merkityn turvallisuusluokitellun tiedon (katso liite I), jonka alkuperäinen luovuttaja on Nato (katso liite II) tai jonka jäsenvaltio toimittaa Natolle,

b. jäsenvaltioiden turvallisuusluokitelluksi merkityn turvallisuusluokitellun tiedon, joka toimitetaan toiselle jäsenvaltiolle Naton ohjelman, hankkeen tai sopimuksen tueksi,

AGREEMENT BETWEEN THE PARTIES TO THE NORTH ATLANTIC TREATY FOR THE SECURITY OF INFORMATION

The Parties to the North Atlantic Treaty, signed at Washington on 4th April, 1949.

Reaffirming that effective political consultation, cooperation and planning for defence in achieving the objectives of the Treaty entail the exchange of classified information among the Parties.

Considering that provisions between the Governments of the Parties to the North Atlantic Treaty for the mutual protection and safeguarding of the classified information they may interchange are necessary.

Realising that a general framework for security standards and procedures is required.

Acting on their own behalf and on behalf of the North Atlantic Treaty Organization,

have agreed as follows:

Article 1

The Parties shall:

(i) protect and safeguard:

(a) classified information (see Annex I), marked as such, which is originated by NATO (see Annex II) or which is submitted to NATO by a member state;

(b) classified information, marked as such, of the member states submitted to another member state in support of a NATO programme, project, or contract,

ii. säilyttävät edellä i alakohdassa määritellyn tiedon turvallisuusluokituksen ja pyrkivät kaikin keinoin turvaamaan tiedon tämän mukaisesti;

(ii) maintain the security classification of information as defined under (i) above and make every effort to safeguard it accordingly;

iii. eivät käytä edellä i alakohdassa määriteltyä turvallisuusluokiteltua tietoa muihin kuin Pohjois-Atlantin sopimuksessa ja siihen liittyvissä päätöksissä ja päätöslauselmissa määrättyihin tarkoituksiin;

(iii) not use classified information as defined under (i) above for purposes other than those laid down in the North Atlantic Treaty and the decisions and resolutions pertaining to that Treaty;

iv. eivät ilmaise edellä i alakohdassa määriteltyä tietoa Natoon kuulumattomille osapuolille ilman tiedon alkuperäisen luovuttajan suostumusta.

(iv) not disclose such information as defined under (i) above to non-NATO Parties without the consent of the originator.

2 artikla

Article 2

Tämän sopimuksen 1 artiklan mukaisesti osapuolet varmistavat kansallisen turvallisuusviranomaisen perustamisen Naton toimintaa varten toteuttamaan suojaavia turvatoimia. Osapuolet laativat ja panevat täytäntöön turvallisuusvaatimuksia, joilla varmistetaan turvallisuusluokitellun tiedon yhteinen suojaustaso.

Pursuant to Article 1 of this Agreement, the Parties shall ensure the establishment of a National Security Authority for NATO activities which shall implement protective security measures. The Parties shall establish and implement security standards which shall ensure a common degree of protection for classified information.

3 artikla

Article 3

1. Osapuolet varmistavat, että kaikista niiden kansalaisista, jotka virallisia tehtäviään hoitaessaan tarvitsevat tai saattavat saada pääsyn turvallisuusluokkaan CONFIDENTIAL ja sitä ylempiin turvallisuusluokkiin kuuluvaan tietoon, tehdään asianmukaisesti turvallisuusselvitys ennen kuin he ottavat tehtävänsä vastaan.

(1) The Parties shall ensure that all persons of their respective nationality who, in the conduct of their official duties, require or may have access to information classified CONFIDENTIAL and above are appropriately cleared before they take up their duties.

2. Turvallisuusselvitysmenettelyt suunnitellaan sellaisiksi, että niillä pystytään selvittämään, voiko henkilö hänen lojaliteettinsa ja luotettavuutensa huomioon ottaen saada pääsyn turvallisuusluokiteltuun tietoon ilman, että siitä aiheutuu turvallisuusriski, jota ei voida hyväksyä.

(2) Security clearance procedures shall be designed to determine whether an individual can, taking into account his or her loyalty and trustworthiness, have access to classified information without constituting an unacceptable risk to security.

3. Osapuolet tekevät pyydettäessä yhteistyötä muiden osapuolten kanssa niiden turvallisuusselvitysmenettelyjä suoritettaessa.

(3) Upon request, each of the Parties shall cooperate with the other Parties in carrying out their respective security clearance procedures.

4 artikla

Pääsihteeri varmistaa, että Nato soveltaa tämän sopimuksen kulloinkin sovellettavia määräyksiä (katso liite III).

5 artikla

Tämä sopimus ei millään tavoin estä osapuolia tekemästä muita sopimuksia, jotka liittyvät niiden luovuttaman turvallisuusluokitellun tiedon vaihtamiseen eivätkä vaikuta tämän sopimuksen soveltamisalaan.

6 artikla

a. Tämä sopimus on avoinna allekirjoittamista varten Pohjois-Atlantin sopimuksen osapuolille, ja se ratifioidaan tai hyväksytään. Ratifioimis- tai hyväksymiskirjat talletetaan Amerikan yhdysvaltojen hallituksen huostaan.

b. Tämä sopimus tulee voimaan kolmenkymmenen päivän kuluttua päivästä, jona kaksi allekirjoittajavaltiota on tallettanut ratifioimis- tai hyväksymiskirjansa. Sopimus tulee voimaan kunkin muun allekirjoittajavaltion osalta kolmenkymmenen päivän kuluttua kunkin valtion ratifioimis- tai hyväksymiskirjan tallettamisesta.

c. Niiden osapuolten suhteen, joiden osalta tämä sopimus on tullut voimaan, sopimus korvaa Pohjois-Atlantin liiton osapuolten turvallisuussopimuksen, jonka Pohjois-Atlantin neuvosto hyväksyi asiakirjan D.C.2/7 liitteessä olevan lisäyksen liitteessä A (1 kohta) 19 päivänä huhtikuuta 1952 ja joka myöhemmin sisällytettiin Pohjois-Atlantin neuvoston 2 päivänä maaliskuuta 1955 hyväksymän asiakirjan C-M (55) 15 (final) liitteeseen A (1 kohta).

7 artikla

Tämä sopimus on avoinna liittymistä varten Pohjois-Atlantin sopimuksen uudelle osapuolelle sen valtiosäännön mukaisten menettelyjen mukaisesti. Tämän osapuolen liit-

Article 4

The Secretary General shall ensure that the relevant provisions of this Agreement are applied by NATO (see Annex III).

Article 5

The present Agreement in no way prevents the Parties from making other Agreements relating to the exchange of classified information originated by them and not affecting the scope of the present Agreement.

Article 6

(a) This Agreement shall be open for signature by the Parties to the North Atlantic Treaty and shall be subject to ratification, acceptance or approval. The instruments of ratification, acceptance or approval shall be deposited with the Government of the United States of America;

(b) This Agreement shall enter into force thirty days after the date of deposit by two signatory States of their instruments of ratification, acceptance or approval. It shall enter into force for each other signatory State thirty days after the deposit of its instrument of ratification, acceptance or approval;

(c) This Agreement shall with respect to the Parties for which it entered into force supersede the "Security Agreement by the Parties to the North Atlantic Treaty Organization" approved by the North Atlantic Council in Annex A (paragraph 1) to Appendix to Enclosure to D.C.2/7, on 19th April, 1952, and subsequently incorporated in Enclosure "A" (paragraph 1) to C-M(55)15(Final), approved by the North Atlantic Council on 2nd March, 1955.

Article 7

This Agreement shall remain open for accession by any new Party to the North Atlantic Treaty, in accordance with its own constitutional procedures. Its instrument of

tymiskirja talletetaan Amerikan yhdysvaltojen hallituksen huostaan. Sopimus tulee voimaan kunkin liittyvän valtion osalta kolmenkymmenen päivän kuluttua sen liittymiskirjan tallettamispäivästä.

8 artikla

Amerikan yhdysvaltojen hallitus ilmoittaa muiden osapuolten hallituksille kunkin ratifioimis-, hyväksymis- tai liittymiskirjan tallettamisesta.

9 artikla

Osapuoli voi irtisanoa tämän sopimuksen antamalla kirjallisen irtisanomisilmoituksen tallettajalle, joka ilmoittaa irtisanomisilmoituksesta kaikille muille osapuolille. Irtisanominen tulee voimaan vuoden kuluttua siitä, kun tallettaja on vastaanottanut ilmoituksen, mutta ei vaikuta niihin velvoitteisiin, oikeuksiin tai valtaoikeuksiin, joita osapuolet ovat aiemmin sopineet tai saaneet tämän sopimuksen määräysten perusteella.

Tämän vakuudeksi allekirjoittaneet, hallitustensa siihen asianmukaisesti valtuuttamina, ovat allekirjoittaneet tämän sopimuksen.

Tehty Brysselissä 6 päivänä maaliskuuta 1997 yhtenä englannin- ja ranskankielisenä kappaleena, jonka kaikki tekstit ovat yhtä todistusvoimaiset, joka talletetaan Amerikan yhdysvaltojen hallituksen arkistoon ja josta tämä hallitus toimittaa oikeaksi todistetut jäljennökset kaikille muille allekirjoittajille.

Liite I

Tämä liite on sopimuksen erottamaton osa.

Naton turvallisuusluokiteltu tieto määritellään seuraavasti:

a. "tieto" tarkoittaa missä tahansa muodossa välitettävää tietoa;

accession shall be deposited with the government of the United States of America. It shall enter into force in respect of each acceding State thirty days after the day of the deposit of its instrument of accession.

Article 8

The Government of the United States of America shall inform the Governments of the other Parties of the deposit of each instrument of ratification, acceptance, approval or accession.

Article 9

This Agreement may be denounced by written notice of denunciation by any Party given to the depository which shall inform all the other Parties of such notice. Such denunciation shall take effect one year after receipt of notification by the depository, but shall not affect obligations already contracted and the rights or prerogatives previously acquired by the Parties under the provisions of this Agreement.

In witness whereof the undersigned, duly authorized to this effect by their respective Governments, have signed this Agreement.

Done in Brussels, this 6th day of March, 1997 in a single copy in the English and French languages, each text being equally authoritative, which shall be deposited in the archives of the Government of the United States of America and of which certified copies shall be transmitted by that Government to each of the other signatories.

Annex I

This Annex forms an integral part of the Agreement.

NATO classified information is defined as follows:

(a) information means knowledge that can be communicated in any form;

b. turvallisuusluokiteltu tieto tarkoittaa tietoa tai aineistoa, jonka katsotaan edellyttävän suojaamista luvattomalta paljastamiselta ja joka on turvallisuusluokituksella osoitettu sellaiseksi;

(b) classified information means information or material determined to require protection against unauthorized disclosure which has been so designated by security classification;

c) ”aineisto” sisältää asiakirjat ja myös valmistetut ja valmisteilla olevat koneet, laitteet ja aseet;

(c) the word "material" includes documents and also any item of machinery or equipment or weapons either manufactured or in the process of manufacture;

d) ”asiakirja” tarkoittaa mitä tahansa tallennettua tietoa riippumatta sen fyysisestä muodosta tai ominaisuuksista, mukaan lukien kirjalliset ja painotuotteet; tietojenkäsittelyssä käytettävät kortit ja nauhat; kartat, kaaviot, valokuvat, maalaukset, piirustukset, kaiverrukset, luonnokset, työmuistiinpanot ja –paperit, hiilipaperikopiot ja värinauhat; millä tahansa keinolla tai menettelyllä tehdyt jäljennökset; kaikenlaiset ääni-, puhe- ja magneettitallenteet sekä elektroniset, optiset ja videotallenteet; kannettavat atk-laitteet, joissa on kiinteät tallennusvälineet, ja irrotettavat tietokoneen tallennusvälineet, mutta ei rajoittuen näihin.

(d) the word "document" means any recorded information regardless of its physical form or characteristics, including, without limitation, written or printed matter, data processing cards and tapes, maps, charts, photographs, paintings, drawings, engravings, sketches, working notes and papers, carbon copies and ink ribbons, or reproductions by an means or process, and sound, voice, magnetic or electronic or optical or video recordings in any form, and portable ADP equipment with resident computer storage media, and removable computer storage media.

Liite II

Tämä liite on sopimuksen erottamaton osa.

Tässä sopimuksessa ”Nato” tarkoittaa Pohjois-Atlantin liittoa ja niitä elimiä, joihin sovelletaan joko Ottawassa 20 päivänä syyskuuta 1951 allekirjoitettua sopimusta Pohjois-Atlantin liiton, kansallisten edustajien ja kansainvälisen henkilöstön asemasta tai Pariisissa 28 päivänä elokuuta 1952 allekirjoitettua pöytäkirjaa Pohjois-Atlantin sopimuksen mukaisesti perustettujen kansainvälisten sotilasesikuntien asemasta.

Annex II

This Annex forms an integral part of the Agreement.

For the purposes of the present Agreement, the term "NATO" denotes the North Atlantic Treaty Organization and the bodies governed either by the Agreement on the status of the North Atlantic Treaty Orgnization, National Representatives and International Staff, signed in Ottawa on 20th September, 1951 or by the Protocol on the status of International Military Headquarters set up pursuant to the North Atlantic Treaty, signed in Paris on 28th August, 1952.

Liite III

Tämä liite on sopimuksen erottamaton osa.

Annex III

This Annex forms an integral part of the Agreement.

Sotilaskomentajien kanssa neuvotellaan heidän valtaoikeuksiensa kunnioittamiseksi.	Consultation takes place with military commanders in order to respect their prerogatives.