Ulkoministeriö
Kansallinen turvallisuusviranomainen
Lakimies Ville Salmi

VN/31134/2022
VN/31134/2022-UM-37

29.05.2023

Eduskunta
Puolustusvaliokunta

Hallituksen esitys eduskunnalle tietoturvallisuudesta Pohjois-Atlantin sopimuksen osapuolten välillä tehdyn sopimuksen ja turvallisuussääntöjen hyväksymiseksi ja voimaansaattamiseksi sekä Suomen ja Pohjois-Atlantin liiton kesken vaihdettavan turvallisuusluokitellun tiedon suojaamiseksi tehdyn hallinnollisen järjestelyn ja Pohjois-Atlantin liiton kanssa tehdyn tietoturvallisuussopimuksen irtisanomiseksi HE 4/2023 vp

Eduskunnan puolustusvaliokunta on pyytänyt ulkoministeriöltä asiantuntijalausuntoa otsikossa mainitusta hallituksen esityksestä (HE 4/2023 vp). Ulkoministeriö kiittää mahdollisuudesta lausua asiassa ja esittää lausuntonaan seuraavaa.

Hallituksen esitys on valmisteltu ulkoministeriössä yhdessä puolustusministeriön, oikeusministeriön, Suojelupoliisin, Liikenne- ja viestintävirasto Traficomin sekä pääesikunnan kanssa.

Esityksen sisältö

Pohjois-Atlantin sopimuksen osapuolten välillä vuonna 1997 tietoturvallisuudesta tehty sopimus (jäljempänä myös tietoturvallisuussopimus) on osa Pohjois-Atlantin liiton oikeudellisesti sitovaa sopimuskehikkoa, johon Pohjois-Atlantin sopimukseen liittyvien uusien jäsenmaiden edellytetään sitoutuvan. Pohjois-Atlantin liiton kaikki nykyisen jäsenvaltiot ovat sopimuksen osapuolia. Tietoturvallisuussopimus on myös yksi niistä kuudesta sopimuksesta, joihin Suomi on sitoutunut liittymään 12 kuukauden sisällä Pohjois-Atlantin sopimusta koskevan Suomen liittymiskirjan tallettamisesta. Naton puolelta on pidetty tärkeänä, että Suomen sitoutuminen Naton tietoturvallisuussopimukseen tapahtuisi mahdollisimman pian, ja joka tapauksessa sanotun määräajan kuluessa. Monenvälinen sopimus korvaa Suomen kahdenväliset tietoturvallisuusjärjestelyt Pohjois-Atlantin liiton kanssa.

Tietoturvallisuussopimuksen mukaan tehokas poliittinen neuvottelu, yhteistyö sekä suunnittelu puolustusasioissa sopimuksen tavoitteiden saavuttamiseksi edellyttävät turvallisuusluokitellun tiedon vaihtamista osapuolten välillä. Sen mahdollistaminen edellyttää määräyksiä turvallisuusluokitellun tiedon vastavuoroisesta suojaamisesta ja turvaamisesta, jolla varmistetaan turvallisuusluokitellun tiedon yhteinen suojauksen taso. Sopimus ei aseta osapuolille velvoitteita luovuttaa turvallisuusluokiteltua tietoa.

Tietoturvallisuudella tarkoitetaan kaikkia sellaisia menettelyjä, joiden avulla turvataan informaation sisällön suojaaminen ulkopuolisilta, tiedon muuttumattomuus sekä tiedon käytettävyys. Tietoturvallisuuden varmistamiseksi käytetään erilaisia keinoja, joista tavallisimmat

ovat henkilöstön luotettavuuden ja toimitilojen turvallisuuden varmistaminen, salassapitosäännökset ja tiedon käytön rajoittaminen vain sovittuun tarkoitukseen sekä erilaiset tiedon käsittelyyn ja siirtoon liittyvät menettelytapavaatimukset. Tietoturvallisuusvaatimukset kattavat informaation koko elinkaaren sisältäen tietojen hankkimisen, muokkaamisen, luovutuksen, arkistoinnin ja hävittämisen.

Tietoturvallisuussopimuksessa määritellään Naton ja sen jäsenvaltioiden turvallisuusluokiteltu tieto, johon sopimusta sovelletaan. Keskeisenä lähtökohtana on, että osapuolet säilyttävät heille luovutetun tiedon turvallisuusluokituksen ja pyrkivät kaikin keinoin turvaamaan tietoa. Tietoa ei luovuteta kolmansille osapuolille ilman tiedon luovuttajan suostumusta.

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

Voimassa oleva Suomen ja Pohjois-Atlantin liiton välillä tehty tietoturvallisuussopimus allekirjoitettiin 22.9.1994 Suomen liityttyä Naton rauhankumppanuusohjelmaan. Kahdenvälisellä sopimuksella Suomi sitoutui luokittelemaan ja suojaamaan rauhankumppanuusohjelman puitteissa Natolta saadun aineiston. Sopimusta on täydennetty 3.7.2012 allekirjoitetulla hallinnollisella järjestelyllä, jonka tarkoituksena oli ajantasaistaa vuoden 1994 sopimus siten, että siinä otetaan huomioon vuonna 2004 säädetyn kansainvälisistä tietoturvallisuusvelvoitteista annetun lain (588/2004) säännökset sekä ajantasaistetut turvallisuusmääräykset. Suomen liittyessä Naton monenväliseen tietoturvallisuussopimukseen nämä kahdenväliset tietoturvallisuusjärjestelyt on tarkoitus irtisanoa yhteisymmärryksessä Naton kanssa sekä niiden voimaansaattamislaki kumota.

Taloudelliset vaikutukset

Natoon liittymisestä johtuvia vaikutuksia on selvitetty hallituksen esityksessä HE 315/2022 vp. Natoon liittyminen aiheuttaa kertaluonteisia lisäkustannuksia ja pysyviä kiinteitä kustannuksia muun muassa tietoturvallisuusratkaisuihin, toimitilaturvallisuuteen sekä järjestelmien tarkastus- ja hyväksyntätyöhön liittyen. Natoon liittyvän tiedon käsittelyn mahdollistavan korkeaa turvallisuutta edellyttävän tietojenkäsittely-ympäristön kehittämiskustannusten arvioidaan olevan noin 20 miljoonaa euroa vuosina 2023-2025. Lisäksi tietojenkäsittelytiloihin vaadittavat suojaukset tulevat aiheuttamaan uusia kustannuksia arviolta noin kuusi miljoonaa euroa kohdistuen pääsääntöisesti vuokrauskustannuksiin. Tietoturvallisuussopimus ei kuitenkaan suoranaisesti lisää valtion yhteisen korkeaa turvallisuutta edellyttävän tietojenkäsittely-ympäristön kustannuksia, koska vastaavat vaatimukset ovat olleet voimassa jo kumppanuusaikana.

Taloudellisia vaikutuksia aiheutuu eri hallinnonaloille mm. tietojärjestelmien muutoksista, toimitilaratkaisuista sekä tietojärjestelmien ja toimitilojen auditoinneista. Tietojärjestelmien suunnittelun tuesta, akkreditointiprosessin etenemisestä sekä järjestelmien hyväksynnästä aiheutuu lisäresurssitarpeita myös kansallisena akkreditointiviranomaisena toimivalle Liikenne- ja viestintävirastolle. Kaikkia kustannusvaikutuksia eri hallinnonaloilla ei ole mahdollista arvioida yksityiskohtaisesti tässä vaiheessa.

Vaikutukset viranomaistoimintaan

Keskeisimmät vaikutukset kansalliseen tietoturvallisuuteen syntyvät eri toimintojen järjestämisestä Naton tietoturvallisuusvaatimusten edellyttämälle tasolle. Suomi suojaa Naton turvallisuusluokiteltua tietoa jo nyt Naton turvallisuussääntöjen vähimmäisvaatimusten ja perusperiaatteiden mukaisesti, eikä sitoutuminen uuteen tietoturvallisuussopimukseen muuta tilannetta merkittävästi. Rauhankumppanuuden aikana vakiintuneet tietoturvallisuusprosessit muodostavat toimivan perustan niitä koskevalle kehitystyölle myös jäsenyyden aikana.

Naton turvallisuusluokiteltujen tietojen määrä ja käsittelytarve laajenee Nato-jäsenyyden myötä eri viranomaisiin sekä yrityksiin. Suomi voi Nato-jäsenyyden myötä saada myös Naton korkeimman turvaluokan (COSMIC TOPS SECRET) asiakirjoja, joita ei pääsääntöisesti luovuteta jäsenvaltioiden ulkopuolisille tahoille. Asiakirjojen määrän kasvu, asiakirjojen vastaanottajien piirin laajentuminen ja päätöksenteon nopeudelle asetettavat vaatimukset on otettava huomioon kehitystyössä.

Naton turvallisuustoimisto teki Suomeen 3.-6.6.2022 tarkastusvierailun, jossa arvioitiin Naton turvallisuusluokitellun tiedon suojaamista. Tarkastuksen johtopäätöksen mukaan viranomaisten tulee arvioida ja tarvittavilta osin lisätä Naton luokitellun tiedon suojaamista koskevia resursseja. Tämä koskee nimenomaisesti kansallista turvallisuusviranomaista ja henkilöturvallisuus-selvityksiä, kirjaamohenkilökuntaa, tietojärjestelmien ja sähköisten käsittely-ympäristöjen hyväksymisprosesseja, toimitilaturvallisuutta sekä yritysturvallisuutta. Pääesikunnassa ja Puolustusvoimissa on tunnistettu tarve vahvistaa asiantuntijaresursseja em. osa-alueilla.

Sähköisten tietojenkäsittely-ympäristöjen suunnittelussa ja toteuttamisessa tulee ottaa huomioon eri ministeriöiden, Suomen ulkomaanedustustojen, tasavallan presidentin kanslian sekä virastojen ja erityisesti Puolustusvoimien tarpeet. Asiakirjajakelut tulevat kohdentumaan eri hallinnonaloille, mutta erityisesti määrän kasvu näkyy Puolustusvoimissa sekä ulko- ja puolustusministeriöissä. Kansallisen TL II –ympäristön kehittäminen, joka on hyväksytty myös NATO SECRET –tason turvallisuusluokitellun tiedon käsittelyyn, on välttämätöntä mahdollisimman nopealla aikataululla. Naton turvallisuusluokiteltua tietoa käsittelevien järjestelmien neuvonta-, tarkastus- ja hyväksyntätyön on arvioitu edellyttävän Liikenne- ja viestintävirastossa pysyvästi lisäresursointitarpeita.

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

Lainsäädännön arviointi

Erityissuojattaviin tietoaineistoihin, joihin lasketaan myös Naton turvallisuusluokiteltu tieto, sovelletaan lakia kansainvälisistä tietoturvallisuusvelvoitteista. Lain soveltamisalan piiriin kuuluu myös Suomen viranomaisen tai lain soveltamisalan piiriin kuuluvan elinkeinonharjoittajan laatimat asiakirjat, joista ilmenee Suomeen toimitettuihin erityissuojattaviin tietoaineistoihin sisältyviä tai sellaisista saatavissa olevia tietoja. Lakia ei sovelleta sellaisten asiakirjojen tai niiden osien salassapitoon tai luokitukseen, jotka sisältävät ainoastaan Suomen kansallista tietoa.

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

Suomen viranomaisen hallussa oleviin asiakirjoihin sovelletaan viranomaisten toiminnan julkisuudesta annettua lakia (621/1999), jollei laissa toisin säädetä. Naton turvallisuusluokiteltuihin asiakirjoihin sovelletaan kansainvälisistä tietoturvallisuusvelvoitteista annetun lain erityissäännöstä ehdottomasta salassapidosta, eikä näihin asiakirjoihin kohdistu julkisuuslain

mukaista salassapidon vahinkoedellytyslausekkeiden mukaista arviointia. Naton turvallisuusluokitellut asiakirjat on siten pidettävä salassa, jollei niitä koskevista sopimuksista tai säännöistä muuta johdu.

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. Asiakirjan ollessa Suomen viranomaisen hallussa, arvioidaan kunkin turvallisuusluokkaa vailla olevan asiakirjan julkisuutta tapauskohtaisesti julkisuuslain perusteella.

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. Tämän perusteella salassa pidettäviä voivat olla esimerkiksi kansainvälisen yhteisön tai toimielimen laatimat asiakirjat, jos ne yhteisössä tai toimielimessä ovat salassa pidettäviä (HE 30/1998 vp).

Kansainvälisistä tietoturvallisuusvelvoitteista annettuun lakiin sisältyy kansallisten asiakirjojen tietoturvallisuudesta annetuista säännöksistä poikkeavia säännöksiä. Lain 3 §:n 1 momentissa on kuitenkin yleinen viittaus julkisuuslakiin sekä julkisen hallinnon tiedonhallinnasta annettuun lakiin (906/2019). 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.

Kansainvälisistä tietoturvallisuusvelvoitteista annettu 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 muutostarpeita.

Turvallisuusselvityslaissa (726/2014) säädetään henkilö- ja yritysturvallisuusselvityksen laadinnassa noudatettavasta menettelystä. Lain tarkoituksena on parantaa mahdollisuuksia ennakolta ehkäistä toimintaa, joka voi vahingoittaa valtion turvallisuutta, maanpuolustusta, Suomen kansainvälisiä suhteista, yleistä turvallisuutta tai muuta näihin verrattavaa yleistä etua taikka erittäin merkittävää yksityistä taloudellista etua taikka edellä tarkoitettujen etujen suojaamiseksi toteutettavia turvallisuusjärjestelyjä (1 §).

Henkilöturvallisuusselvityksen laatii Suojelupoliisi, tai Pääesikunta, jos selvityksen kohde toimii tai hänen on tarkoitus toimia puolustusvoimissa tai hoitaa puolustusvoimien antamaa tehtävää taikka jos turvallisuusselvitys liittyy puolustusvoimien toimintaan tai hankintoihin. Yritysturvallisuusselvityksen laatii Suojelupoliisi, taikka Pääesikunta, 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.

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, että Suo-

men ja Naton väliseen hallinnolliseen järjestelyyn sisältyvät määräykset loivat riittävästi edellytyksiä henkilötietojen suojaa koskevien vaatimusten huomioimiselle julkisuus- ja salassapitonäkökohtien ohella.

Naton tietoturvallisuussopimuksen ei katsota vaativan asiasisältöisen lainsäädännön muuttamista. Sopimus ja Naton turvallisuussäännöt ehdotetaan voimaansaatettavaksi näin ollen ns. blankettilailla.

Eduskunnan tiedonsaantioikeus

Eduskunnan tiedonsaanti- ja osallistumisoikeus Nato-asioissa turvataan perustuslain ja muun lainsäädännön nojalla. Parlamentaarisen järjestelmän toimintaan kuuluu välttämättömänä elementtinä tiedonkulku eduskunnan ja hallituksen välillä. Sovellettavia sääntöjä selostetaan yksityiskohtaisemmin hallituksen esityksen jaksossa 2.4.

Vaiteliaisuusmenettely ja Naton turvallisuussääntöjen mukaisten toimintamallien, mukaan lukien tila-, henkilöstö- ja tiedonhallintaratkaisut, sekä niihin liittyvien teknisten ratkaisujen noudattaminen mahdollistavat asianmukaisen tiedonkulun eduskunnalle jatkossakin. Käytännön järjestelyistä on käyty keskusteluja eduskunnan turvallisuustoimiston ja valiokuntasihteeristön ja kansallisen turvallisuusviranomaisen sekä määrätyn turvallisuusviranomaisen välillä hallituksen esityksen valmistelun aikana.