Poliisihallitus

Lausunto

21.04.2023 POL-2023-40655

Asia: VN/31134/2022

Luonnos hallituksen esitykseksi eduskunnalle tietoturvallisuudesta Pohjois-Atlantin sopimuksen osapuolten välillä tehdyn sopimuksen ja turvallisuussääntöjen hyväksymiseksi ja voimaansaattamiseksi ja Suomen ja Pohjois-Atlantin liiton kesken vaihdettavan tu

Lausunnonantajan lausunto

Voitte kirjoittaa lausuntonne alla olevaan tekstikenttään

lausunto 21.4.2023 POL-2023-40655

Poliisihallituksen lausunto hallituksen esityksestä koskien NATO:n tietoturvallisuussopimuksia

Ulkoasianministeriö on pyytänyt lausuntoa luonnoksesta hallituksen esitykseksi eduskunnalle tietoturvallisuudesta Pohjois-Atlantin sopimuksen osapuolten välillä tehdyn sopimuksen ja turvallisuussääntöjen hyväksymiseksi ja voimaansaattamiseksi ja Suomen ja Pohjois-Atlantin liiton (Nato) kesken vaihdettavan turvallisuusluokitellun tiedon suojaamiseksi tehdyn hallinnollisen järjestelyn ja Pohjois-Atlantin liiton kanssa tehdyn tietoturvallisuussopimuksen irtisanomiseksi (viite: VN/31134/2022). Lausuntopyyntö on julkaistu lausuntopalvelussa ja lausuntojen määräaika on 21.4.2023.

Suomi liittyi Pohjois-Atlantin liittoon 4.4.2023. Tämän seurauksena Suomi sitoutui myös liittymään tietoturvallisuudesta Pohjois-Atlantin sopimuksen osapuolten välillä tehtyyn sopimukseen vuoden sisällä. Tämä monenvälinen sopimus korvaa Suomen kahdenväliset tietoturvallisuusjärjestelyt Naton kanssa.

1.1 Poliisin huomiot hallituksen esityksestä

Poliisihallitus katsoo, että kokonaisuudessaan asia on selkeä. Hallituksen esitys koskee Suomen ja Naton rauhankumppanuuden yms. vuoksi solmittujen sopimusten irtisanomista samalla, kun Suomen pitää hyväksyä täysjäsenenä Naton monikeskeiset turvallisuussäännöt.

Poliisihallitus haluaa tuoda esille sen, ettei poliisin tietojen käsittely ja tietoturvallisuus ole kaikilta osin Naton turvallisuussäännöstöjen mukaista, koska poliisi on noudattanut kansallisia normeja. Tämä johtuu siitä, että poliisi ei ole ollut säännönmukaisesti Natosta saapuvien asiakirjojen vastaanottajana ja arkistonmuodostajana kuten esim. ulkoasiainministeriö ja puolustusvoimat. Kansalliset turvallisuusvaatimukset poikkeavat jonkin verran Naton vastaavista. Jatkossa Natosta saapuvien asiakirjojen jakelu tulee todennäköisesti laajenemaan ja poliisin pitää mukauttaa tietojen käsittelyä ja turvallisuustoimenpiteitään uusien määräysten mukaisiksi. Tämä vaatii aikaa ja resursseja.

Turvallisuussopimuksen lisäksi muut sopimukset, joihin Suomen jäsenenä pitää liittyä, koskevat esimerkiksi Naton jäsenvaltioiden joukkojen asemaa, Naton sotilasesikuntien asemaa, keksintöjen salassapitoa ja puolustuksen alan teknistä tietoa.

Liittyminen Naton puolustussuunnitteluprosessiin ja siinä Suomelle kohdistettavien suorituskykytavoitteiden toimeenpanoon sekä osallistumiseen Naton operatiiviseen suunnitteluun on tunnistettu aiheuttavan merkittäviä lisäkustannuksia, joita on mahdollista arvioida vasta myöhemmin. Kustannuksia aiheutuu mm. Naton rauhan ajan tehtävistä, monikansallisista suorituskykyhankkeista, johtamisjärjestelmistä ja valmiusvaatimuksista, jotka koskenevat myös poliisia. Suomen Nato-jäsenyyteen sisältyy edellä esitettyjen lisäksi lyhyellä aikavälillä toteutuvia kertaluonteisia lisäkustannuksia ja

pysyviä kiinteitä kustannuksia mm. tietoturvallisuusratkaisuihin ja toimitilaturvallisuuteen liittyen sekä näihin kytkeytyviin henkilöresursseihin. Taloudellisia vaikutuksia tulee arvioida osana julkisen talouden suunnitelmien sekä talousarvioesitysten laatimista. Kaikkia kustannusvaikutuksia ei ole mahdollista arvioida yksityiskohtaisesti tässä vaiheessa.

Suomen liittyminen Natoon vaikuttaa ennen kaikkea Suomen ulko-, turvallisuus- ja puolustuspolitiikkaan. Näin ollen Nato-jäsenyyden merkittävimmät vaikutukset kohdistuvat pääasiassa puolustushallintoon ja ulkoasiainhallintoon. Nato-jäsenyyden vaikutus muihin valtionhallinnon sektoreihin on rajallinen, mutta poliisin ollessa keskeinen sisäisen turvallisuuden toimija tulee vaikutuksia myös poliisiin. Naton työ kriisinsietokyvyn parissa liittyy kansalliseen siviilivalmius- ja varautumistyöhön, koska suomalaisen kokonaisturvallisuuden mallin toimeenpano on koko valtionhallinnon vastuulla. Tämän vuoksi on oletettavaa, että myös poliisille tulee jatkossa enenevässä määrin Naton asiakirjajakeluita ja kertyy Naton tietoja.

Naton turvallisuustoimiston Suomeen toukokuussa 2022 tekemän 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. Poliisissa samoin kuin puolustusvoimissa on tunnistettu tarve vahvistaa asiantuntijaresursseja edellä mainituilla osa-alueilla. Poliisihallitus voi yhtyä hallituksen esitykseen siinä, ettei Nato-asiakirjojen määrän kasvua voida vielä tässä vaiheessa arvioida. Erityisesti asiakirjojen käsitte lyyn ja jakeluun tarvittavaa kirjaamohenkilökunnan lisäystarvetta ja sen kustannuksia ei hallituksen esityksessä ole riittävästi otettu huomioon. Hallituksen esityksessäkin todetaan, että käsittelytarpeen laajenemista eri viranomaisiin on vaikea ennustaa. Tämä koskee erityisesti poliisihallintoa, joka ei ole ennen jäsenyyttä käsitellyt laajamittaisesti Nato-tietoja, eikä ole ollut Nato-asiakirjojen ns. ala-arkistonmuodostajana Suomessa kuten esim.

Pääesikunta.

Hallituksen esitykseen sisältyvissä asiakirjoissa korostuu aiemmin Suomessa varsin vähän esiin tuotu sisäpiiriuhkan olemassaolon huomiointi ja sen tarkoituksenmukainen kontrollointi, mihin hallituksen esityksen perusteella osallistuu jatkossa Naton turvallisuustoimisto yhdessä toimivaltaisten kansallisten viranomaisten ja Naton sotilas- ja siviilielinten kanssa. Sisäpiiriuhkan kontrollointi ei ole enää vain kansallisten viranomaisten asia, vaan Nato -tietoa koskien myös Naton toimielinten toimivaltuuksiin kuuluva asia. Tämä toimivaltuuksien muutos pitää jatkossa ottaa huomioon kansallisessa

organisaatiossa ja niiden normeissa, jotka käsittelevät Naton asiakirjoja.

Riskienhallintaa ei saa käyttää keinona kiertää Naton määrittämiä turvallisuusperiaatteita. Tämä tarkoittanee käytännössä sitä, ettei Naton sopimuksessa asettamista turvallisuusvaatimuksista voitane poiketa Nato-tietoa käsittelevissä organisaatioissa tukeutuen kansallisiin riskienhallinta keinoihin. Riskienhallinnan keinojen pitäisi olla ensin hyväksytetty kansallisen turvallisuusviranomaisen (NSA) tai sen toimeksiannosta määrätyn turvallisuusviranomaisen (DSA) toimesta. Hallituksen esitykseen sisältyvistä asiakirjoista ei voida kuitenkaan ilman tarkempaa perehtymistä päätellä rajanvedosta tai

siitä, milloin NSA/DSA osallistuvat riskienhallinnan keinojen hyväksyttävyyden arviointiin osana prosessia.

Jäsenyyden alkuvaiheessa Suomessa ongelmaksi voi muodostua Naton turvaluokiteltujen tietojen käsittely tietojärjestelmissä siltä osin, kun tietojärjestelmät pitäisi tähän tarkoitukseen arvioida Liikenne- ja viestintäviraston hyväksymän arviointilaitoksen toimesta. Toistaiseksi arviointilaitoksia ei ole hyväksytty tekemään EU:n tai Naton turvallisuusluokiteltuja tietoja käsittelevien tietojärjestelmien arviointeja (hallituksen esitys sivu 11). Mikäli asiakirjoja käsitellään vain paperiasiakirjoina, täytyy perusteluna käyttää tiedonhallintalain 19 §. Turvallisuusviranomaisten TUVE-ympäristössä, myös poliisissa on käsitelty sähköisesti myös kansallista turvaluokiteltua tietoa. Nato-tietojen ja asiakirjojen osalta käsittely pitäisi ottaa uuteen tarkasteluun Suomen jäsenyyden myötä. Tarvitaan pikaisesti hyväksyttyjä arviointilaitoksia ja käytännön tason ohjeistusta siitä, missä

laajuudessa turvaluokiteltuja Nato-asiakirjoja voidaan käsitellä sähköisesti ja missä järjestelmissä (Hallituksen esityksessä kustannukset sivu 17). Lisääntyvä asiakirjaliikenne Suomen ja Naton välillä ja alempiin turvaluokkatasoihin kuuluvien asiakirjojen laajamittainen käsittely paperisena ei tue tehokasta asiakirjahallintaa ja

Suomen digitalisaatiolle 2030 asettamia tavoitteita (Suomen digitaalinen kompassin, VN julkaisu 2022:65).

Asiakirjoissa korostetaan muun ohella turvallisuuskoulutus- ja tietoisuusohjelmaa sekä tietoturvaloukkauksista ilmoittamista Naton tiedonhallinta- ja Naton turvallisuusperiaatteet mukaisesti. Tämä tarkoittaa käytännössä sitä, että Naton toimielimille on mahdollistettava selkeä näkyvyys Nato-tiedon käsittelyyn ja turvallisuusvaatimusten mukaisiin hallintatoimenpiteisiin. Tämä lisää Naton valvontatoimielimien tietoa kansallisten Nato-tietoa käsittelevien organisaatioiden sisäisistä turvallisuus- ja varautumismenettelyistä järjestelmien toimivuudesta. Menettely tulee monille Suomen organisaatioille uutena. Poliisiin kohdistuva kansainvälinen ulkopuolinen valvonta on ollut ennen Natoa suhteellisen vähäistä. Poikkeuksena tästä on ollut valvonnan kohdistuminen yksittäisiin tietojärjestelmiin, joilla on vaikutuksia esimerkiksi Europolin laajuisiin kokonaisuuksiin. Aiemmin kansalliseen organisaatioiden omaan riskienhallintaan perustuvia ratkaisuja ei voida enää Nato-tiedon osalta ottaa perustaksi, vaan ratkaisun hyväksyttävyys tulee perustua ulkopuoliseen arvioon.

Mikäli kansallisella organisaatiolla on hallussaan Naton turvaluokiteltua tietoa, asettaa Nato myös varautumisvelvoitteita. Tältä osin menettelyt linkitty vät vahvasti myös kansallisten organisaatioiden sisäiseen valmiussuunnitteluun ja varautumiseen erilaisiin normaaliolojen häiriötilanteisiin sekä poikkeusoloihin. Velvoite laajentaa kansallisten organisaatioiden ja toimijoiden varautumisvelvoitteita entisestään ja lisää kustannuksia. Lisäksi näiden velvoitteiden mukaista toimintaa myös kontrolloidaan aiempaa laajemmin Nato -toimielinten toimesta tai niiden valtuuttamana NSA/DSA -viranomaisten toimesta.

Asiakirjoissa korostetaan Nato-tiedon suhdetta medialle ja tiedonvälityskanaville annettavaan tietoon, mitä tuleekin tarkastella suhteessa julkisuuslain soveltamiseen sekä sen ehdotonta salassapitoa sekä julkisuus- ja salassapito-olettaman mukaisiin salassapitosäännösten vaatimuksiin. Vaikka Nato-asiakirjoihin voidaan varsin laajasti soveltaa salassapitosäännöksiä, pitäisi myös julkisuuslakia tarkistaa Suomen Nato -jäsenyyden myötä. Turvaluokitellun tiedon osalta kansallinen säännöstö tukee Naton asiakirjojen käsittelyä. Ongelmia julkisuuslain tulkinnassa saattaa tulla erityisesti

NATO, UNCLASSIFIED (NU) luokiteltujen asiakirjojen osalta (Hallituksen esityksen sivu 8) sekä osittain salassa pidettävien asiakirjojen osalta (vert. Naton tietoturvallisuussäännöt liite E, kohta 12). Lisäksi Naton tietoturvallisuussäännöissä on kohtia, jotka voivat edellyttää myös hankintalainsäädännön uudistamista joltakin osin (ks. Naton tietoturvallisuussäännöt liite G.)

Asiakirjoissa korostetaan teknisten suojausratkaisujen riskin määrittämistä koskevan vastuun koordinointia teknisten asiantuntijoiden kanssa. Toisaalta todetaan, että näissäkin tapauksissa päätöksenteko ratkaisuista kuuluu asianmukaiselle turvallisuusviranomaiselle, mikä poistaa tällöin kansallisten organisaatioiden oman tai yksinomaan niiden omaan riskienhallintaan perustuvan arvioinnin. Asiakirjoissa todetaan selkeästi, että Naton jäsenvaltioiden tulee muun muassa käyttää vain sellaisia laitteita, jotka asianmukainen turvallisuusviranomainen on hyväksynyt Naton turvallisuusluokitellun tiedon suojaamiseen.

Lisäksi korostetaan tietoturvallisuuden täydentämistä henkilöstöturvallisuudella, toimitilaturvallisuudella sekä viestintä- ja tietojärjestelmien turvallisuudella, jotta varmistetaan tasapainoinen toimenpiteiden kokonaisuus Naton turvallisuusluokitellun tiedon suojaamiseksi (esim. hajasäteilyturvallisuuden toteuttaminen kaikissa toimitiloissa vaatii Suomessa lisäarviointia). Jos tulokulma tietojen suojaamisesta muutettaessa esimerkiksi laajempaan organisaatioturvallisuuteen, painotettavat turvallisuuden osa-alueet voivat muuttua ja painottua eri tavoin. Tämä ilmeneekin osittain muun muassa fyysisiä turvallisuusvaatimuksia tarkastelevassa osuudessa. Lisäksi on tärkeä ottaa huomioon se, että tietosuojakysymykset pyritään ratkaisemaan sopimus- ja sääntelytasolla siten, että tietojen käsittely on kaikissa tilanteissa selkeää ja sujuvaa.

Kokonaisuudessaan hallituksen esityksen osalta on syytä arvioida edellä esitettyjen näkökulmien lisäksi sitä, kuinka laajasti Suomen julkishallinnossa tullaan jatkossa käsittelemään Nato-tietoa ja asiakirjoja. Puolustussuunnittelu on Suomessa ollut perinteisesti koko yhteiskunnan läpileikkaava prosessi ja kaikilla tasoilla kunnista yrityksiin asti. Tämän vuoksi on

perusteltua arvioida, voidaanko kansalliset nykyiset tietoturvallisuusnormistot mukauttaa ja hienosäätää nopeasti niin, että ne vastaisivat Naton turvallisuussäännöstöjä tarpeellisilta osin. (Esim. turvallisuusselvitysten osalta lainsäädäntöä on syytä tarkistaa ja ohjeistusta tulee vaatimaan esim. se, miten Nato-tietoihin kohdistuvista tietoturvapoikkeamista Suomen osalta

ilmoitetaan Naton turvallisuustoimistolle.) Kansallisten tietoturvallisuuteen liittyvien normien yhdenmukaistaminen Naton säännöstön kanssa helpottaisi tietoturvallisuutta ylläpitävien toimijoiden normiston soveltamiseen liittyviä tehtäviä ja pienentäisi tietoturvariskejä, koska soveltamisessa ei tarvitsisi noudattaa kahdenlaisia käytäntöjä. Myös Naton tietoturvallisuussäännöt vaativat Suomen jäsenyyden jälkeen päivittämistä (vert. Liite H kohta 3). Tästä Suomen Nato-edustusto pitänee huolen.

Poliisihallituksella ei ole esittää hallituksen esitykseen muita huomioita. Toivomme lain pikaista voimaantuloa, jotta Suomen Nato jäsenyyden edellyttämät lainsäädäntömuutokset saatetaan voimaan ajoissa. Lisäksi toivomme, että lausuntokierroksella saatu palaute otetaan huomioon.

Poliisijohtaja Janne Paavola

Ryhmäpäällikkö Marja Piiroinen-Honkanen

Asiakirja on sähköisesti allekirjoitettu asianhallintajärjestelmässä. Poliisi

21.04.2023 klo 13:48. Allekirjoituksen oikeellisuuden voi todentaa kirjaamosta.

Jakelu Lausuntopalvelu

Tiedoksi Poliisihallituksen Esikunta, Vesa Wickström

Piiroinen-Honkanen Marja
Poliisihallitus - Poliisihallituksen Esikunta