Huld Oy

Lausunto

27.11.2023

Asia: VN/18157/2023

Lausuntopyyntö: luonnos hallituksen esitykseksi kyberturvallisuusdirektiivin (NIS2-direktiivi) täytäntöönpanemiseksi

Lausunnonantajan lausunto

Yleiset huomiot NIS2-direktiivin tavoitteista ja tarkoituksesta

Tavoite vahvistaa EU:n yhteistä ja jäsenvaltioiden kansallista kyberturvallisuuden tasoa kriittisiksi katsottujen sektoreiden ja toimijoiden osalta asettamalla velvoittavia riskienhallintatoimia kyberturvallisuushäiriöiden varalta on ehdottoman kannatettava. Eri valtioiden tapa implementoida herättää toki kysymyksiä: tuleeko implementointitavoista liian erilaisia, jolloin useammassa maassa toimivalle taholle muodostuu liiallista tulkintaa ja byrokratiaa.

Tavoitteen yhdenmukaisen toteutumisen voidaan arvioida riippuvan siitä, miten selvästi vaatimukset pystytään implementoimaan, kuinka hyvin toimijat hyväksyvät ja sisäistävät edellytetyt toimet ja miten tehokkaasti toteutettuja riskienhallinnan toimenpiteitä pystytään valvomaan. Huomiota tulisi kiinnittää toimijoiden yhdenvertaiseen kohteluun riippumatta direktiivin implementoivasta jäsenvaltiosta tai toimijan asemasta julkisena tai yksityisenä toimijana.

Säädöstyön lähtökohta, että siinä noudatetaan NIS2-direktiivin edellyttämää vähimmäistasoa velvoitteiden soveltamisalan, laajuuden ja valvonnan suhteen, kuitenkin kansallista liikkumavaraa täysimääräisesti hyödyntäen, on hyvä.

Soveltamisalaa koskevat huomiot

EI ko

Riskienhallintavelvoitetta koskevat huomiot

Riskienhallinnassa tulisi noudattaa kaikki vaaratekijät huomioivaa lähestymistapaa ja varmistaa, että yrityksen hallintotapa ja riskienhallintaprosessit ottavat huomioon kyberturvallisuusriskit.

"Kaikki vaaratekijät" on absoluuttinen muotoilu. Vastaava “kaikki”-sanan käyttö aiheutti aikanaan tulkintaepäselvyyksiä myös sosiaali- ja terveydenhuollon asiakastietojen käsittelyä koskevan lain (Asiakastietolaki) voimaan tullessa (termi "Kaikki potilastiedot"). Sanamuoto tulee suoraan direktiivistä, joten se ei liene muutettavissa, mutta on otettava huomioon se, että ”Tärkeät toimijat” eivät ole ennakkovalvonnan alaisia, joten riskienhallinnan kattavuutta (onko “kaikki” vaaratekijät huomioitu riittävästi) arvioitaneen mahdollisissa jälkikäteisvalvonnoissa. Pidämme todennäköisenä, että ainakin jotkut Julkishallinnon toimijat tulevat pyytämään etukäteisohjeistusta siitä, mikä on riittävä luettelo “kaikista vaaratekijöistä”. Esimerkkinä tällaisesta voisi mahdollisesta olla ENISA Threat taxonomy?

Lain kyberturvallisuuden riskienhallinnasta ehdotetun 8 § perusteluissa (HE s. 119) on laajempi kuvaus kaikki vaaratekijät huomioivan lähestymistavan sisällöstä kuin ehdotetussa Tiedonhallintalain 18 b § perusteluissa (HE s. 161). Molempien perustelutekstien tulisi olla samansisältöiset, jotta vältytään tulkintaongelmilta niiden Julkishallinnon toimijoiden kohdalla, jotka tuottavat palveluita myös muilla NIS2-toimialoilla. Esimerkkinä Hyvinvointialueet (Julkishallinto ja Terveys).

Raportointivelvoitetta koskevat huomiot

Yhdenmukaisuus ja selkeys

Yhtenäisen raportointikanavankin toteuttamisen kannalta olisi hyvä, että pykälien ja momenttien järjestys ja sanamuoto olisivat mahdollisimman yhteneväiset julkisen hallinnon tiedonhallinnasta (906/2019) ja kyberturvallisuuden riskienhallinnasta annetuissa laeissa.

Merkittävä poikkeama

“Poikkeama katsotaan merkittäväksi, jos se on aiheuttanut tai voi aiheuttaa palvelujen vakavan toimintahäiriön tai asianomaiselle toimijalle taloudellisia tappioita tai jos poikkeama on vaikuttanut tai voi vaikuttaa muihin luonnollisiin henkilöihin tai oikeushenkilöihin aiheuttamalla huomattavaa aineellista tai aineetonta vahinkoa.”

”Taloudelliselle tappiolle” ei ole määritetty laadullisia kriteereitä, kuten ”toimintahäiriölle” ja ”vahingolle”. Sanamuodon mukaisesti tulkiten, jo mahdollisuus pienenkin taloudellisen tappion aiheutumisesta täyttäisi merkittävän poikkeaman määritelmän.

Valvontaa koskevat huomiot

Yhdenmukaisuuteen, ennustettavaan soveltamiseen sekä viranomaisten välisten vastuiden selkeyteen on kiinnitettävä erityistä huomiota niiden valvovien viranomaisten kohdalla, joiden kohteena on sama valvottava organisaatio. Esimerkkinä Hyvinvointialue, joka on sekä Julkisen sektorin että Terveys –toimialan toimija.

Seuraamusmaksua koskevat huomiot

Perustuslakivaliokunta on vakiintuneesti katsonut hallinnollisten seuraamusmaksujen olevan lainvastaisesta teosta määrättäviä sanktioluonteisia hallinnollisia seuraamuksia ja rinnastanut ne asiallisesti rangaistusluonteisen taloudellisen seuraamuksen rikosoikeudelliseen seuraamukseen.

Ehdotetussa laissa onkin viitteitä seuraamusten rikosoikeudellisen luonteen huomioimisesta. Muun muassa syyksiluettavuus edellyttää tahallisuutta tai törkeää huolimattomuutta, sanktion määräämättä jättäminen on sidottua harkintaa, sanktioista päättää ainakin muodollisesti monijäseninen elin, kaksoisrangaistavuus samasta teosta on kielletty ja seuraamusmaksu pannaan täytäntöön kuten sakko.

Seuraamusmaksu voidaan ehdotuksen mukaan määrätä muun muassa riskienhallinnan toimenpiteiden toteuttamisen laiminlyönnistä. Kun konkreettiset riskien hallintatoimenpiteet ovat harkinnanvaraisia ja tulee suhteuttaa toimijan alaan, toimintaan ja sen riskeihin, voidaan kysyä, säädetäänkö laissa riittävän täsmällisesti, tarkkarajaisesti ja tyhjentävästi teosta tai laiminlyönnistä, joka voisi olla toimijaan kohdistuvan seuraamusmaksun määräämisen perusteena.

Huomioidaanko asiassa lisäksi syyttömyysolettama ja itsekriminointisuoja, erityisesti suhteessa monitasoisiin sanktioihin, pakkokeinoihin ja valvovan viranomaisen laajaan tiedonsaantioikeuteen salassapitomääräysten estämättä? Onko toimijan, esimerkiksi tietoja luovuttamalla, edistettävä mahdollisen rikkomuksen selvittämistä ja täten seuraamusmaksun määräämistä?

CSIRT-yksikön tehtäviä koskevat huomiot

Ei kommentoitavaa

Tiedonhallintalakia ja täytäntöönpanoa julkishallinnossa koskevat huomiot

Esimerkiksi Hyvinvointialueen on järjestettävä riskienhallintansa sekä Tiedonhallintalain (Julkishallinto) että uuden lain kyberturvallisuuden riskienhallinnasta (Terveys) mukaisesti. Käytännön kannalta olisi tärkeää, että pykälien ja momenttien järjestys ja sanamuoto olisivat mahdollisimman yhteneväiset Tiedonhallintalaissa ja laissa kyberturvallisuuden riskienhallinnasta. Nyt mm. TiHL 18b § on molemmat "Kyberturvallisuuden riskienhallintavelvoite ja riskienhallinnan toimintamalli", kun taas ehdotetussa riskienhallintalaissa on erikseen 7 § "Kyberturvallisuuden riskienhallintavelvoite" ja 8 § "Kyberturvallisuuden riskienhallinnan toimintamalli"

Tiedonhallintalain 4a luvun ja lain kyberturvallisuuden riskienhallinnasta kanssa 2 luvun rakenteen ja sisällön yhtenäistäminen helpottaisi Hyvinvointialueen yhteistyötä yksityisten Terveystoimialan, sekä kansainvälisten toimijoiden kanssa, kun ei tarvitsisi varmistaa sanamuotoja sekä Tiedonhallintalain että lain kyberturvallisuuden riskienhallinnasta (ja NIS2 direktiivin) kanssa.

Lain kyberturvallisuuden riskienhallinnasta ehdotetun 8 § perusteluissa (HE s. 119) on laajempi kuvaus kaikki vaaratekijät huomioivan lähestymistavan sisällöstä kuin ehdotetussa Tiedonhallintalain

18 b § perusteluissa (HE s. 161). Molempien perustelutekstien tulisi olla samansisältöiset, jotta vältytään tulkintaongelmilta niiden Julkishallinnon toimijoiden kohdalla, jotka tuottavat palveluita myös muilla NIS2-toimialoilla. Esimerkkinä Hyvinvointialueet (Julkishallinto ja Terveys).

Lakiesitysluonnokseen kyberturvallisuuden riskienhallinnasta ei sisälly mahdollista asetuksenantovaltuutusta standardien käytöstä. Tiedonhallintalain kohdalla tällainen mahdollisuus on mainittu (HE luonnos s. 232). Voiko tästä aiheutua, että esimerkiksi Hyvinvointialueelle kohdistuisi standardien käyttövaatimus Tiedohallintalain kautta, mutta se ei kohdistuisi Terveystoimialaan?

Verkkotunnusvälittäjiä koskevat huomiot

Ei kommentoitavaa

Kumottavaksi ehdotettuja säännöksiä koskevat huomiot

Ei kommentoitavaa

Vaikutustenarviointia koskevat huomiot

Ei kommentoitavaa

Muut huomiot ja avoin palaute esityksestä

Ehdotetun lain terminologia vaikuttaa harkitulta ja yhdenmukaiselta implementoitavan direktiivin kanssa. On kuitenkin huomionarvoista, että näin ei ole kaikkien asiaa koskettavien lakien tai standardien ja parhaiden käytäntöjen kanssa, joihin kyberturvallisuuden riskienhallinnan toimintaperiaatteiden ja toimintamallin olisi suositeltavaa perustua. Esimerkkinä voidaan mainita ”poikkeama” tai vastaavan sisältöisen termin käyttö esitysluonnoksessa, ISO27001 ja ISO27002 standardeissa sekä laissa sosiaali- ja terveydenhuollon asiakastietojen käsittelystä.

Filander Mika
Huld Oy

Kellomäki Tarmo
Huld Oy - Turvallisuuskonsultointia tuottavan yksikön kootut kommentit.