Vantaan ja Keravan hyvinvointialue

Lausunto

29.11.2023

Asia: VN/18157/2023

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

Lausunnonantajan lausunto

Yleiset huomiot NIS2-direktiivin tavoitteista ja tarkoituksesta

Vantaan ja Keravan hyvinvointialue kiittää mahdollisuudesta kommentoida luonnosta hallituksen esitykseksi NIS2-direktiivin täytäntöönpanemiseksi.

Direktiivin tavoitteena on vahvistaa kansallisen kyberturvallisuuden tasoa kriittisten toimijoiden osalta asettamalla näille uusia velvoitteita mm. riskienhallinnan osalta ja seuraamuksia velvoitteiden laiminlyönnistä.

Yleisenä huomiona esitys on pääosin oikeilla linjoilla tarpeesta valvoa, varautua ja velvoittaa organisaatioita toimiin tietoturvansa kehittämiseksi. Näiden toteutumisen seuranta ja tukeminen voi kuitenkin olla haasteellista, mikäli onnistumisen kriteereitä ei ole riittävän tarkasti määritelty.

Vantaan ja Keravan hyvinvointialue toteaa lisäksi yleisenä kommenttina, että hallituksen esityksen mukaisten lakiluonnosten velvoitteet keskeisille toimijoille, kuten hyvinvointialueet, lisäävät huomattavasti hallinnollista taakkaa ja kustannuksia, joita taloudellisesti haasteellisessa asemassa olevat hyvinvointialueet eivät ole riittävällä tasolla huomioineet valmistelussa ja talouden suunnittelussa.

Soveltamisalaa koskevat huomiot

Hyvinvointialueiden käytännön toiminnassa ja palveluita järjestettäessä eri toimialoja on haastavaa erottaa toisistaan. Toiminnallisesti sosiaali- ja terveydenhuollon ja pelastustoimen integraatio haastaa toimialajaon. Tulisiko terveydenhuoltoa ja sosiaalihuoltoa käsitellä eri toimialojen kautta? Kuinka käsitellään tilanteita, joissa sosiaalihuollossa kirjataan terveydenhuollon rekisteriin? Mitä toimintoja hyvinvointialueelta toimialatulkinnan kautta kuuluu julkishallinnon toimialaan? Millaisia

riskienhallinnan toimenpiteitä tulee hyvinvointialueen ulottaa kyberturvan näkökulmasta sen järjestämisvastuulla oleviin palveluketjuihin ja sen toimijoihin esim. sopimusjohtamisen kautta?

Miten pelastustoimen palvelut tulee tässä yhteydessä ymmärtää, kun pelastustoimi hyödyntää palvelutoiminnassa osittain TUVE-verkkoa, jonka toimijat eivät ole NIS2 direktiivin parissa? Osittain taas pelastustoimen tietojärjestelmät toimivat hyvinvointialueen verkoissa. Pelastustoimi käsityksemme mukaisesti kuulunee NIS2 direktiivin pariin ollen mahdollinen CER-direktiivin mukainen toimija, mutta ainakin yleisesti osana hyvinvointialuetta julkishallinnon toimialan kautta. Tuleeko pelastustoimi erottaa omaksi toimialakseen, jos se on CER-toimija vai riittääkö se, että sitä käsitellään julkishallinnon kokonaisuudessa?

Vantaan ja Keravan hyvinvointialue NIS2 toimijana ymmärryksemme mukaan näyttäytyy direktiivin soveltamisessa seuraavasti:

- Terveystoimiala (koskenut jo aiemmin), keskeinen toimija, valvova viranomainen Valvira

- Julkishallinnon toimiala (uusi toimiala), tärkeä toimija, valvova viranomainen liikenne- ja viestintävirasto

Direktiivissä kyseiset toimialat ovat erilaisia suhteessa toisiinsa erityisesti valvonnan näkökulmasta. Eroja on mm. ennakkovalvonnan, seuraamusmaksujen, toiminnan rajoittamistoimenpiteiden sekä uhkasakkojen osalta. Direktiivi itsessään ei kerro, miten toimialarajat voidaan organisaatiossa ymmärtää, jolloin kyse on soveltamisesta. Siksi on syytä tarkentaa viranomaisyhteistyötä ja toimialojen rajoja yhdessä hyvinvointialueiden kanssa.

Riskienhallintavelvoitetta koskevat huomiot

Lakiluonnoksessa kyberturvallisuuden riskienhallinnasta todetaan, että valvova viranomainen voi toimialallaan antaa tarkempia teknisiä määräyksiä koskien riskienhallintaa. Tähän liittyen milloin artiklan 21 kyberturvallisuusriskien hallintatoimenpiteiden ja kontrollien vaatimukset tarkentuvat? Kuinka paljon nämä tulevat tarkentumaan?

Raportointivelvoitetta koskevat huomiot

Lakiluonnoksen kyberturvallisuuden riskienhallinnasta 11 §:n mukainen 24 h raportointivelvollisuus merkittävistä poikkeamista vaatii määrittämään toimijalle varallaoloprosessit.

Raportointivelvollisuuksien täyttäminen vaatii muutoksia ja resursseja toimijoiden prosesseihin sekä lisää siitä aiheutuvia kustannuksia.

Lisäksi olemassa oleviin hankintasopimuksiin tulee neuvotella muutoksia lain vaatimista riskienhallinta- ja raportointivelvoitteista. Tämä aiheuttaa lisäkustannuksia ja sopimusmuutoksia

sekä mahdollisesti hankinnan kilpailuttamista uudelleen, mikäli sopimusmuutokset eivät ole hankintalain sallimia sopimusmuutoksia.

Valvontaa koskevat huomiot

Vantaan ja Keravan hyvinvointialue kuuluu keskeisiin toimijoihin, ja täten Vake kuuluu etukäteis- ja jälkikäteisvalvonnan piiriin. Tämä tarkoittaa sitä, että viranomaisilla on valtuudet esimerkiksi suorittaa erilaisia tarkastuksia ja auditointeja. Tuleeko valvovan viranomaisen ilmoittaa etukäteen tarkastusten tai auditointien ajankohdasta toimijalle?

Määräytyykö Vaken valvova viranomainen julkishallinnon vai terveysalan mukaisesti? Eli onko Vaken valvova viranomainen Kyberturvallisuuskeskus (Liikenne- ja viestintävirasto) vai Valvira (Sosiaali- ja terveysalan lupa- ja valvontavirasto)?

Seuraamusmaksua koskevat huomiot

Hallituksen esityksessä ehdotetaan säädettäväksi ”ettei NIS2-direktiivin hallinnollisia seuraamusmaksuja voitaisi määrätä julkishallinnon toimijoille.”

Lakiluonnoksessa kyberturvallisuuden riskienhallinnasta todetaan, että seuraamusmaksua ei voida määrätä valtion viranomaisille, valtion liikelaitoksille, kunnallisille viranomaisille, itsenäisille julkisoikeudellisille laitoksille, eduskunnan virastoille, tasavallan presidentin kanslialle eikä Suomen evankelisluterilaiselle kirkolle ja Suomen ortodoksiselle kirkolle eikä niiden seurakunnille, seurakuntayhtymille ja muille elimille.

Lakiluonnoksessa ei kuitenkaan mainita hyvinvointialueita. Vantaan ja Keravan hyvinvointialue kysyy, koskevatko seuraamusmaksua koskevat määräykset myös hyvinvointialuetta?

CSIRT-yksikön tehtäviä koskevat huomiot

Ei kommentteja

Tiedonhallintalakia ja täytäntöönpanoa julkishallinnossa koskevat huomiot

”Julkisia sosiaali- ja terveydenhuollon palveluntuottajia ovat vuoden 2023 alusta lähtien olleet hyvinvointialueet, joiden NIS2-direktiiviin perustuvista riskienhallinta- ja raportointivelvoitteista säädettäisiin tiedonhallintalaissa osana julkisen sektorin velvoitteita.” Tulevatko hyvinvointialueita koskettavat NIS2-direktiivin kaikki vaatimukset olemaan tiedonhallintalaissa?

Verkkotunnusvälittäjiä koskevat huomiot

Ei kommentteja

Kumottavaksi ehdotettuja säännöksiä koskevat huomiot

Ei kommentteja

Vaikutustenarviointia koskevat huomiot

Onko vaikutustenarvioinnista tulossa tarkemmat ohjeistukset?

Muut huomiot ja avoin palaute esityksestä

Terminologiaan olisi hyvä kiinnittää huomiota siten, että hallituksen esityksessä käytetty termistö tarkistettaisiin siten, että se mahdollisimman hyvin vastaisi Suomessa jo tehtyä tietoturvan sanastotyötä. Tämä helpottaisi käytännön toteutuksia organisaatiossa ja edistäisi lainsäädännön yhteentoimivuutta.

Liljeroos Riikka
Vantaan ja Keravan hyvinvointialue - Konsernipalvelujen toimialajohtaja
29.11.2023