Hallintovaliokunta torstai 05.09.2024 klo 12.15 / HE 57/2024 vp

Hyvil dnron 92/03.01.01/2024.

Hyvinvointialueyhtiö Hyvil Oy:n lausunto hallintovaliokunnalle luonnoksesta hallituksen esitykseksi kyberturvallisuusdirektiivin (NIS2-direktiivi) täytäntöönpanemiseksi

Kiitämme mahdollisuudesta tulla kuulluksi luonnoksesta hallituksen esitykseksi kyberturvallisuusdirektiivin (NIS2-direktiivi) täytäntöönpanemiseksi.

Direktiivin tarkoitus vahvistaa ja yhdenmukaistaa kyberturvallisuustasoa tietyillä yhteiskunnan sektoreilla koko EU-laajuisesti on hyvä asia. Yhtenäiset vähimmäistasoiset velvoitteet kyberturvallisuuden riskienhallinnasta ja merkittävien poikkeamien raportoinnista selkeyttävät ja edistävät kyberturvallisuustoimenpiteitä organisaatioissa.

Useita lausuntokierroksella esille tuomiamme epäselviä kohtia on tähän hallituksen esitykseen korjattu tai ne ovat huomioitu (esim. johdon toiminnan rajoittaminen, seuraamusmaksut). Edelleen haluamme kuitenkin nostaa esiin muutamia seikkoja käytännön toimeenpanon näkökulmasta.

Hyvinvointialueiden lähtökohdat NIS2 direktiiviin

Hyvinvointialueille siirtyi 1.1.2023 vastuu järjestää sosiaalihuollon, terveydenhuollon ja pelastustoimen palvelut. Aiemmat terveydenhuollon toimijat (mm. sairaanhoitopiirit) ovat pääsääntöisesti olleet jo NIS1 direktiivin piirissä ja siten kyberturvallisuuden riskienhallinta on tästä näkökulmasta osalle toimijoista jo tuttua. Organisaatioina hyvinvointialueet ovat kuitenkin vielä nuoria ja soveltajina uusia toimijoita.

Taustaselvityksestä kävi ilmi, että tietosuojaan liittyvät toimenpiteet ovat terveydenhuoltoalaan kohdistuvan regulaation myötä hoidettu, mutta kyberturvallisuuden osalta monen toimijan kohdalla arvioitiin tarvittavan järjestelmällisempiä toimenpiteitä. Erityisesti kriittisten palveluiden suojaaminen sekä toimitusketjut, joissa palveluntarjoajien kyberturvallisuuden tason seuraaminen ja sopimusvelvoitteiden asettaminen arvioitiin heikoksi.

Kyberturvallisuuslain säännöskohtaisissa perusteluissa todetaan, että (Säännöskohtaiset perustelut s. 140) *”että silloin kun lain liitteessä I tai II tarkoitettua toimintaa harjoittaa oikeushenkilö, kattaisi tässä laissa tarkoitettu toimijan määritelmä silloin kyseisen oikeushenkilön kokonaisuutena. Edellä todetulla tavalla toimijan määritelmää olisi tulkittava oikeussubjektikohtaisesti. Lain ja siinä säädettyjen velvoitteiden soveltaminen ei siten olisi tarkoitus rajoittua ainoastaan liitteissä tarkoitettua toimintaa harjoittavaan yksikköön tai toimintoon oikeushenkilössä, vaan velvoitteet koskisivat kyseistä oikeushenkilöä sellaisenaan, eli toimijaa kokonaisuutena. Esimerkiksi oikeushenkilö joka toimii usealla toimialalla, joista vain osa on mainittu lain liitteissä, kuuluisi siten sääntelyn piiriin myös sellaisten toimintojen osalta, joita ei ole mainittu lain liitteissä. Poikkeuksena tästä olisi kuitenkin myöhemmin 4 §:ssä säädetyt rajoitukset lain soveltamisalaan.”* **Selvää on, että hyvinvointialue kokonaisuutena on NIS2 soveltamisen piirissä, mutta epäselvää on, miten eri soveltamisalojen osalta tulee yhden hyvinvointialueen sisällä toimia ja miten valvonta tähän suhteutuu.**

Hyvinvointialueet kuuluvat ymmärryksemme mukaan direktiivin toimialaan sekä jo aiemmin toimialaluettelossa olleen terveydenhuoltotoimialan kautta, mutta jatkossa myös muiden toimialojen kautta. Pääasiallisesti direktiivin toimeenpano tehdään säätämällä uusi kyberturvallisuuslaki, mutta julkishallinnon toimialan osalta säädökset viedään täydennyksenä tiedonhallintalakiin.

Olemme tunnistaneet, että joissakin tilanteissa yksittäinen hyvinvointialue voisi kuulua NIS2 soveltamisalaan kaikkien tai osan näistä toimialoista kautta. Selkeää on, että hyvinvointialueet ovat NIS2 toimijoita vähintään Terveydenhuoltoalan kautta (kyberturvallisuuslaki) ja julkisen hallinnon toimialan kautta (tiedonhallintalaki). Lisäksi osa HVAista toimii lääkinnällisten laitteiden valmistajina ja niillä on sairaala-apteekkeja. Hieman epäselväksi jää, tuleeko hyvinvointialueet soveltamisalaan myös pelastuslaitosten kautta (CER-direktiivin mukaisena kriittisenä toimijana) tai luetaanko jokin osa yliopistosairaaloiden tekemästä tutkimuksesta tai hyvinvointialueiden muusta tutkimuksesta NIS2 tutkimustoiminnan soveltamisalaan.

Soveltaminen hyvinvointialueiden toiminnassa

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?

Hyvinvointialue NIS2 toimijana

Ymmärryksemme mukaan hyvinvointialue näyttäytyy direktiivin soveltamisessa seuraavasti:

- Terveystoimiala (koskenut jo aiemmin), keskeinen toimija, valvova viranomainen Valvira
- Julkishallinnon toimiala (uusi toimiala), tärkeä toimija, valvova viranomainen liikenne- ja viestintävirasto
- Lääkinnällisten laitteiden osalta valmistustoimiala (uusi toimiala), keskeinen toimija, valvova viranomainen Fimea
- Apteekkitoimiala (uusi toimiala), keskeinen toimija, valvova viranomainen Fimea
- Epäselviä toimialoja ovat pelastustoimi (julkishallinto/CER-direktiivi), jonka valvova viranomainen olisi molemmissa tapauksissa liikenne- ja viestintävirasto sekä tutkimustoiminta, jonka valvova viranomainen olisi liikenne- ja viestintävirasto.

  Tutkimustoiminnan osalta tulkitsemme, että HVAt tuskin kuuluvat soveltamisalaan, koska pääsääntöisesti ne toimivat opetus- ja koulutusalan laitoksina. Tätä voitaisiin kuitenkin vielä tarkentaa, jotta lain tulkinnasta ja lainsäätäjän tarkoituksesta ei jäisi epäselvyyttä.

Direktiivissä kyseiset toimialat ovat erilaisia suhteessa toisiinsa erityisesti valvonnan näkökulmasta. HE on selkiytynyt siten, että seuraamusmaksuja tai johdon toiminnan rajoittamistoimenpiteitä ei voitaisi määrätä hyvinvointialueille, joka on mielestämme hyvä ja selkiyttävä asia.

Eroja toimialojen välillä on edelleen mm. ennakkovalvonnan, toiminnan rajoittamistoimenpiteiden sekä uhkasakkojen sekä määräaikojen (kyberturvallisuuslaki vs. tiedonhallintalaki) 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.

Käytännön haasteita tulkinnan osalta voi tulla mm. siinä, millaiset koulutukset ovat organisaatioissa riittäviä. Tärkeää olisikin, että koulutusten tarkoitus ja tavoitteet olisivat selkeitä ja koulutusten suuntaaminen riittävän yksiselitteistä, jotta organisaatioiden on mahdollista toteuttaa direktiiviä oikean tasoisesti.

Hyvinvointialueiden valvonta

Usean toimialan kautta direktiivin soveltamisalaan kuuluminen herättää kysymyksiä. Direktiivissä monitoimialaorganisaatioissa valvotaan organisaatioita toimialoittain, eli jokaista toimialaa valvoo kyseisen toimialan valvova viranomainen. Tiedonhallintalaki puolestaan viittaa tiedonhallintayksikköön, ja sitä kautta herääkin kysymys siitä, miten toimialat direktiivin puitteissa tulee rajata suhteessa toisiinsa? Mikä esimerkiksi on hyvinvointialueen julkishallinnon toimialaa? Toimialakohtaista valvontaa tukee ymmärrys valvottavasta toimialasta, joka on hyvä perustelu ehdotettuun kansalliseen malliin, mutta jättää avoimia kysymyksiä.

Tuleeko hyvinvointialueita tulkita tässä yhteydessä siten, että terveystoimiala tulee erottaa omaksi toimialakseen, valmistustoimiala omakseen ja kaikki muut hyvinvointialueen toiminnot kuuluvat julkishallinnon toimialaan? Miten tämä käytännössä voidaan toteuttaa organisaatiossa, jossa palvelutoimintaa pyritään nimenomaisesti integroimaan? Erityisen tärkeää on, että hyvinvointialueilla ja valvovilla viranomaisilla on jatkossa yhteinen ymmärrys siitä, miten toimialakohtainen valvonta kohdistuu hyvinvointialueen toimintoihin ja mikä viranomainen valvoo mitäkin kohdealuetta ja antaa soveltamisesta ohjeita.

Pidämme tärkeänä, että soveltamista ja valvontaa selkeytetään tilanteessa, jossa organisaatio kuuluu NIS2 direktiivin piiriin useamman toimialan kautta. Kaikissa tilanteissa hyvinvointialueisiin kohdistuvan viranomaisten valvonnan tulee olla yhteismitallista ja velvoitteiden toteutumisesta tehtävien tulkintojen selkeitä ja yhtenäisiä silloinkin, kun valvovia viranomaisia on useita. Lisäksi ohjeistuksen tulee olla yhtenäistä kaikille hyvinvointialueille, Helsingin kaupungille (kun se hoitaa sote-tehtäväänsä) ja hyvinvointiyhtymille. **Nyt hallituksen esityksestä käy ilmi, että viranomaisten yhteistyölle ei olla osoittamassa lisäresursseja, vaan se nähdään asiaksi, joka voidaan hoitaa nykyisillä resursseilla siitä huolimatta, että NIS2 valvontaan on tulossa täysin uusia viranomaistahoja, joilla ei ole kokemusta NIS1 soveltamisesta.**

Emme pidä järkevänä tilannetta, jossa hyvinvointialueet pyytävät ohjeita eri valvontaviranomaisilta tai keskustelevat erikseen valvontaviranomaisten kanssa tulkinnoista ennakkoon tai valvontatoimenpiteiden yhteydessä. Viranomaisvalvonnan yhtenäisyyteen, yhteismitallisuuteen ja valvovien viranomaisten yhteistyöhön tulee kiinnittää erityistä huomiota. Tämä tulee tehdä kansallisesti yhteistyössä, kuten kyberturvallisuuslain 26§ velvoittaa.

Hallituksen esityksessä viranomaisille esitetään erillisiä omia valvontaan liittyviä järjestelmiä ja useassa yhteydessä todetaan, että valvottava organisaatio toimittaa tietoja valvontaa tekevälle organisaatiolle. Esim. kyberturvallisuuslain 9§ eriyttää valvovien viranomaisten erillisen mahdollisuuden ohjeistaa, samoin poikkeamailmoitusten osalta 11§ antaa mahdollisuuden erillisiin ilmoitusmenettelyihin. Tätä tukee eri viranomaisille suunniteltujen valvontajärjestelmien määrä. **Voitaisiinko ilmoittaminen ja rekisteritiedot kuitenkin toteuttaa keskitetysti ja asiakaslähtöisesti sen sijaan, että valvoville viranomaisille toimitetaan erilliset ilmoitukset ja ne sitten ilmoittavat keskitetylle yhteispisteelle sen tarvitsemat tiedot? Tämä edistäisi myös sitä, että koordinaatiota tosiasiallisesti tapahtuu valvovien viranomaisten välillä.**

- ➔ valvovien viranomaisten yhteystyön ja koordinaation toimimattomuudella on suoria vaikutuksia hyvinvointialueisiin kohdistuviin valvontatoimiin ja niiden yhteismitallisuuteen. Erityisesti soveltamisen alkuvaiheessa tulee kiinnittää huomiota siihen, että hyvinvointialueiden kaltaisten useammasta näkökulmasta valvottavien toimijoiden valvonnan järjestämiseen, rajoihin ja yhteisiin ohjeisiin kiinnitetään riittävää huomiota.
- ➔ Ehdotamme, että Liikenne- ja viestintäviraston koordinaatiovastuuseen kiinnitetään riittävästi resursseja, jotta yhteistyölle saadaan toimivat kehykset, ohjeet ja yhtenäiset toimintamallit
- ➔ Hyvinvointialueiden näkökulmasta on kestämätöntä, jos eri valvovat viranomaiset kohdistavat valvontatoimenpiteitä eri tavoilla, tasoilla ja eriaikaisesti organisaatioon ja sen toimintaan.
- ➔ Osa valvontaviranomaisista on uusia toimijoita, joilla ei ole NIS1 valvontavelvollisuutta. Osaamisen kehittämiseksi tukea tarvitaan Liikenne- ja viestintävirastolta.

Muita huomioita

Lisäksi on hyvä huomata, että Suomessa sosiaali- ja terveydenhuollon asiakastietolaissa ja sen asetuksissa on samankaltaista sääntelyä, jota osittain muokataan tämän direktiivin osalta, mutta myös THL:n määräyksistä löytyy sääntelyä tietoturvaan ja kyberturvaan liittyen jatkossakin mm. sosiaalihuollon osalta.

Ilmoittautumismenettelyn osana tulee jatkossa ilmoittaa IP-osoitealueet valvovalle viranomaiselle sekä ylläpitää kyseistä tietoa. Pilvipalveluiden käyttö on lisääntynyt myös julkishallinnossa ja sotessa, sillä pilvipalveluiden käytön on todettu parantavan julkisen hallinnon tietoturvaa. Pilvipalveluiden IP-osoitealueiden muutoksista voi tulla jatkossa organisaatioille kohtuullisen aikaa vievää, mikäli palveluntarjoajat muuttavat niitä useasti. Tähän tulee kehittää lomakepohjasta poikkeava tiedonsiirtotapa (esim. rajapinta), mikäli tarve osoittautuu suureksi.

Pidämme hyvänä, että kansallista liikkumavaraa on käytetty siten, että direktiivin soveltamista ei ole laajennettu vähimmäistasosta ja mahdollisuuksien mukaisesti on huomioitu julkisen hallinnon organisaatioiden ominaispiirteet myös seuraamuksia määrittäessä.

Kuten nykytilaa koskevassa jaksossa 3.16 on kuvattu, voimassa oleva tiedonhallintalain sääntely kattaa osin jo nykyisellään kyseiset direktiivin mukaiset velvoitteet. Samassa yhteydessä todetaan, että kyberturvallisuusriskien noudattaminen ei lisää tiedonhallintayksiköiden työtä, koska samantasoisia velvoitteita on jo ollut tiedonhallintalaissa. Käytännössä kuitenkin kyberturvallisuuden eriyttäminen omaksi osiokseen (nyt osana tietoturvallisuutta) vaatii hallinnollista työtä ja toiminnan muutoksia organisaatioissa. Tässäkin tarvitaan selkeitä ohjeita NIS2 piirissä oleville tiedonhallintayksiköille.

Nostamme tässä vielä esiin hyvinvointialueiden omistamien ns. inhouse-yhtiöiden kuulumisen osin NIS2 soveltamisalaan. Osa yrityksistä kuuluu soveltamisalaan CER-toimijoina (ruokapalvelutoimijat) ja osa mm. lääkinnällisten laitteiden valmistajina tai laboratoriopalveluita tarjoavina toimijoina. Näiden toimijoiden osalta tulisi vielä harkita seuraamustoimenpiteiden oikeellisuutta tilanteessa, jossa toimijat käytännössä toimivat julkisella rahalla tarjoten palveluita omistajilleen. **Esimerkiksi seuraamusmaksut tulisivat käytännössä omistajien maksettaviksi.** Hyvinvointialueet omistavat valtion kanssa erillistoimialayhtiö DigiFinland Oy:n joka tullee osaksi soveltamisalaa ja jonka osalta seuraamustoimenpiteitä tulisi myös harkita.

Hyvinvointialueiden tulee kattaa NIS2 direktiivin toimeenpanosta syntyvät kustannukset yleiskatteellisesta rahoituksestaan. Iso osa toimijoista joutuu sitomaan suuren osan tietoturvaan ja tietosuojaan varatusta rahoitusosuudesta NIS2 toimeenpanoon ja kyberturvallisuuden tason nostamiseen. Rahoituksen käyttäminen tarkoituksenmukaisiin toimenpiteisiin ja todellisen kyberturvallisuuden tason nostoon vaatii yhtenäisiä ja yhdenmukaisia ohjeita valvovilta viranomaisilta sekä koulutusta & tukea näiden ohjeiden ja mahdollisten kriteerien noudattamiseen.

Kyberturvallisuudesta kertyvää tietoa ja oppeja tulisi kyetä tehokkaasti jakamaan myös hyvinvointialueille, jotta kyberturvallisuudet taso tosiasiallisesti nousee.