Terveyden ja hyvinvoinnin laitos THL

Lausunto

24.11.2023

Asia: VN/18157/2023

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

## Lausunnonantajan lausunto

**Yleiset huomiot NIS2-direktiivin tavoitteista ja tarkoituksesta**

THL kannattaa esitettyjä tavoitteita ja riskienhallintalähtöisyyttä.

Ehdotus- ja perustelumateriaalissa tulisi korjata harhaanjohtava termi "turvallisuussuunnitelma" ja korvata se asiakastietolain mukaisella termillä "tietoturvasuunnitelma".

**Soveltamisalaa koskevat huomiot**

Soveltamisala -kohta on puutteellinen, huomioiden sosiaali- ja terveydenhuollon keskeiset toimijat.

THL toivoo täsmennystä sosiaali- ja terveydenhuollon toimijoista käytettäviin termeihin, joiden tulisi olla yhteneväisiä asiakastietolain 703/2023 mukaisesti. Keskeisiä toimijoita ovat sekä yksityiset että julkiset sosiaali- ja terveyspalvelujen järjestäjät ja tuottajat eli palvelunantajat. Myös ja erityisesti sosiaalipalvelujen tarjoajat ja apteekit tulisi ottaa huomioon ehdotetussa laissa.

Sekä valvonnan yhtenäistämiseksi että eri säädösten ristiriitaisuuden vähentämiseksi "Terveyssektori" tulisi korvata sosiaali- ja terveyspalveluja kuvaavilla termeillä läpi materiaalin. Esimerkiksi Valviran valvonta ei rajoitu pelkästään terveyspalveluihin.

Terveyssektorin perusteluteksteissä on virheellisesti kuvattu, että vain julkisen terveydenhuollon yksiköiden olisi velvoite liittyä Kanta-palveluihin. Liittymisvelvoite koskee kaikkia julkisen ja yksityisen sektorin sote-palvelunantajia, joilla on sähköinen järjestelmä asiakastietojen käsittelyyn. Kyseinen velvoite koskee myös apteekkeja.

Ehdotuksen mukaan valvovan viranomaisen valvontatoimivaltuuksia ja tiedonsaanti- sekä tarkastusoikeutta ei sovellettaisi tasavallan presidentin kansliaan, valtioneuvoston oikeuskanslerin toimintaan eikä Kansaneläkelaitokseen. Ehdotuksen mukaan ”Rajoitukset johtuvat pääosin näiden julkiseen sektoriin kuuluvien organisaatioiden perustuslaissa säädetystä asemasta, jonka perusteella valtion keskushallintoon kuuluvien viranomaisten ohjaustoimivaltaa ei voida ulottaa näiden organisaatioiden sisäisen hallinnon ohjaukseen (esim. PeVL 46/2010).”

PeV on kuitenkin todennut myöhemmässä käytännössään (PeVL 14/2018) seuraavaa: ”Perustuslakivaliokunnan käsityksen mukaan on kuitenkin selvää, että kansallista valtiosäännön rakenteisiin kiinnittyvää identiteettiä koskeva sopimusmääräys voi muodostaa vain kapeasti sovellettavissa olevan oikeasuhtaisen perusteen poiketa EU-oikeuden täysimääräisestä soveltamisesta. Unionin tuomioistuimen vakiintuneessa oikeuskäytännössä on katsottu, että unionin oikeuden ensisijaisuuden periaatteen, joka on unionin oikeusjärjestyksen olennainen ominaisuus, mukaan se, että jäsenvaltio vetoaa kansallisen oikeutensa säännöksiin, edes perustuslain tasoisiin säännöksiin, ei voi heikentää unionin oikeuden vaikutusta tämän jäsenvaltion alueella (ks. mm. asia 11/70, Internationale Handelsgesellschaft, tuomio 17.12.1970, 3 kohta ja asia C 409/06, Winner Wetten, tuomio 8.9.2010, 61 kohta ja erityisesti asia C-399/11, Melloni, tuomio 26.2.2013, k. 59). ”

PeV:in lausunnon perusteella vaikuttaisi siltä, että perustuslaista johtuvia rajoituksia valvovan viranomaisen toimintaan olisi mahdollista kohdistaa vain oikeuskanslerin toimintaan, ellei NIS2-direktiivistä tunnisteta jotain muuta perustetta rajoituksille.

**Riskienhallintavelvoitetta koskevat huomiot**

Ei lausuttavaa.

**Raportointivelvoitetta koskevat huomiot**

Raportointivelvoitteen aikarajat voivat olla haastavia tilanteissa, joissa toimijalla ei ole aktiivista valvontaa 24/7 periaatteella. Raportointivelvoitteen täyttäminen vaatii käytännössä organisaatioita suorittamaan 24/7 valvontaa joko itse tai ulkoistettuna palveluna. Lisäksi merkittävän poikkeaman määritelmänä on mm. palvelujen vakava toimintahäiriö – on epäselvää, tarkoitetaanko tällä lähinnä julkisia palveluita vai koskeeko vaatimus myös ns. sisäisiä palveluita.

**Valvontaa koskevat huomiot**

Asiakastietolain 703/2023 90 § 2 momentti: ”Palvelunantajan, apteekin, Kansaneläkelaitoksen ja tietojärjestelmäpalvelun tuottajan tai tietojärjestelmän valmistajan tai välittäjän on ilmoitettava viipymättä Sosiaali- ja terveysalan lupa- ja valvontavirastolle sellaisesta sen käyttämiin käyttöympäristöihin ja tietoverkkoihin kohdistuvasta merkittävästä tietoturvallisuuteen liittyvästä häiriöstä, jonka seurauksena tietojärjestelmien käyttö ja sosiaali- ja terveyspalveluiden toteuttaminen voi merkittävästi vaarantua. Terveyden ja hyvinvoinnin laitos voi antaa tarkempia määräyksiä siitä, milloin häiriö on merkittävä, sekä ilmoituksen sisällöstä, muodosta ja toimittamisesta.”

THL:n mandaatti asiakastietolaissa liittyy sote-tietojärjestelmien olennaisiin vaatimuksiin, sisältäen myös olennaiset tietoturvavaatimukset. Nämä vaatimukset keskittyvät kuitenkin vaatimustenmukaisuuden osoittamiseen ennen järjestelmien tuotantokäyttöä eikä operatiivisiin häiriöihin tai niiden hallintaan. Asiakastietolaissa oleva THL:n mandaatti merkittävien häiriöiden määräämisestä on päällekkäinen ehdotetun NIS-sääntelyn kanssa.

Asiakastietolain 82 § 1 momentti tietojärjestelmien olennaisten vaatimusten merkittävistä poikkeamista helposti sekoittuu esitetyn lain 11 §:n 5 momentin valvontaviranomaisen valtuuteen antaa tarkempia teknisiä määräyksiä tietoverkoissa ja käyttöympäristössä havaituista merkittävistä poikkeamista. THL kannattaa asiakastietolain 90 pykälän muuttamista siten, että tietoverkkoihin ja käyttöympäristöihin liittyvät poikkeamat määrätään NIS2-säädösten perusteella.

Käyttöympäristöön ja operatiiviseen verkkoympäristöön liittyvistä poikkeamista määrääminen ei ole luonteva osa olennaisten vaatimusten ja niiden poikkeamien sääntelyä, koska olennaiset vaatimukset kohdistuvat eri käyttöympäristöissä käytettäviin tietojärjestelmätuotteisiin.

**Seuraamusmaksua koskevat huomiot**

Ehdotuksen mukaan julkinen hallinto aiotaan jättää seuraamusmaksujen ulkopuolelle. NIS2-direktiivin mukainen seuraamusmaksu on kopio EU:n yleisen tietosuoja-asetuksen mukaisesta seuraamusmaksusta. Tietosuojalakia säädettäessä käytettiin kansallista liikkumavaraa ja julkishallinnon toimijat jätettiin seuraamusmaksun ulkopuolelle. Julkisen hallinnon jättäminen GDPR-seuraamusmaksujen ulkopuolelle on kuitenkin osoittautunut käytännössä toimimattomaksi ja epäoikeudenmukaiseksi, koska esim. virkavastuu voi kohdistua satunnaisesti yksittäiseen virkamieheen organisaation sijasta tai samalla toimialalla organisaatioita kohdellaan eri tavoin (esim. ammattikorkeakoulut voivat saada sakkoja, mutta yliopistot eivät). Myös tietosuojavaltuutettu on todennut nykyisen järjestelyn toimimattomaksi ja hallitusohjelman mukaisessa tietosuojalainsäädännön kokonaisuudistuksessa on tarkoitus säätää GDPR-seuraamusmaksut tietosuojaloukkauksista koskemaan julkista ja yksityistä sektoria yhtäläisesti. Olisikin harkitsematonta, tehotonta ja hallinnollisesti sekavaa valita käytännössä huonoksi todettu vaihtoehto.

**CSIRT-yksikön tehtäviä koskevat huomiot**

Ei lausuttavaa.

**Tiedonhallintalakia ja täytäntöönpanoa julkishallinnossa koskevat huomiot**

Ei lausuttavaa.

**Verkkotunnusvälittäjiä koskevat huomiot**

Ei lausuttavaa.

**Kumottavaksi ehdotettuja säännöksiä koskevat huomiot**

Ei lausuttavaa.

**Vaikutustenarviointia koskevat huomiot**

Toimijan velvollisuus huolehtia henkilöstön osaamisesta on ilmeinen ja voi vaatia lisäresursointia, jolloin erityisesti pienillä toimijoilla voi olla haasteita velvoitteen ja osaamisen täyttämiseksi. Näin ollen olisi tärkeää laatia toimintamalleja ja ohjeistusta ja erinäisiä tukiverkkoja osaamisen jakamiseksi ja kasvattamiseksi. CSIRT toimijana voisi olla tässä tärkeässä roolissa.

**Muut huomiot ja avoin palaute esityksestä**

Ei lausuttavaa.

Rintamaa Janne
Terveyden ja hyvinvoinnin laitos THL