Sosiaali- ja terveysalan lupa- ja valvontavirasto Valvira

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

-

Soveltamisalaa koskevat huomiot

Lain soveltamisala ja Valviran toimivalta

Luonnoksessa hallituksen esitykseksi ehdotetaan lakia kyberturvallisuuden riskienhallinnasta (jäljempänä kyberturvallisuuslaki), jossa säädettäisiin yhteiskunnan toiminnan kannalta kriit-tisten toimijoiden kyberturvallisuuden riskienhallinta- ja raportointivelvoitteista. Valviran oh-jaus- ja valvontatoimivalta koskisi ehdotuksen mukaisesti terveydenhuoltoalan toimijoita, jot-ka on lueteltu lain liitteen I kohdan 13 alakodissa a–e.

Valvira toteaa, että Valviran valvontavastuulle ehdotetut tahot on määritelty liian laajasti, sillä niihin kuuluisivat terveydenhuollon palveluntuottajien lisäksi Lääkealan turvallisuus- ja kehit-tämiskeskus Fimean toimivaltaan tällä hetkellä kuuluvat toimijat (EU:n vertailulaboratoriot, lääkkeiden tutkimusta, kehitystä ja valmistusta harjoittavat toimijat sekä vakavan kansanter-veysuhan aikana kriittisiksi katsottuja lääkinnällisiä laitteita valmistavat toimijat). Valvira eh-dottaa edellä liitteen I kohdan 13 alakodissa b–e alakohdissa mainittujen toimijoiden säätä-mistä Fimean valvontavastuulle. Nykyisten säädösten nojalla Valvira ohjaa ja valvoo valta-kunnallisesti terveydenhuollon palveluntuottajia. Valvira toteaa, että ehdotetussa kyberturval-lisuuslaissa tulee säätää Valviran valvontatoimivallasta nykyistä sääntelyä vastaavalla, joka koskee ainoastaan terveydenhuollon tarjoajia.

Terveydenhuollon digitalisaation ja potilaille tarjottavien etäpalveluiden laajentumisen sekä valmisteilla olevan eurooppalaisen terveysdata-avaruuden perustamista koskevan asetuksen (EHDS-

asetus) myötä NIS2-direktiivin mukaiset häiriötilanteet ja valvonta-asiat voivat jatkos-sa liittyä enenevässä määrin tilanteisiin, joissa on kyse rajat ylittävästä terveydenhuollon pal-velutoiminnasta. Ehdotuksen 6 §:ssä (lainkäyttövalta ja alueellisuus) säädettäisiin, että val-vova viranomainen voi suorittaa toiseen Euroopan unionin jäsenvaltioon sijoittautuneeseen toimijaan kohdistuvia valvonta- tai täytäntöönpanotoimia, jos toisen jäsenvaltion toimivaltai-nen viranomainen sitä pyytää ja toimija tarjoaa palveluja Suomessa tai sillä on viestintäverk-ko tai tietojärjestelmä Suomen alueella. Edellytyksenä on lisäksi, että valvovalla viranomai-sella olisi oikeus suorittaa vastaava valvonta- tai täytäntöönpanotoimi tämän lain nojalla, jos toimija olisi sijoittautunut Suomeen.

Valvira toteaa, että sillä on toimivalta valvoa Suomeen sijoittautuneita terveydenhuollon pal-veluntuottajia ja tehdä esimerkiksi näiden toimitiloihin tarkastuksia. Edellä ehdotettu rajat ylit-täviä valvonta-asioita koskeva toimivaltasäännös on ongelmallinen, sillä se ei selkeästi ota kantaa muun muassa siihen, millä kriteereillä toimijan sijoittautumista johonkin valtioon arvi-oidaan sekä mikä on pykälän tarkoittamissa tilanteissa kansallisen valvontaviranomaisen ja sijaintivaltion valvontaviranomaisen välinen toimivallan jako ja käytettävissä olevat valvonta-keinot. Valvira ehdottaa sääntelyä täsmennettäväksi rajat ylittävien häiriö- ja valvontatilantei-den osalta. Edelleen valmistelussa on syytä täsmentää miten NIS2-direktiivi ja ehdotettu ky-berturvallisuuslaki suhteutuvat terveydenhuollon toimijoiden osalta niin sanottuun EU-potilasdirektiiviin (2011/24/EU) ja sen mukaiseen hoitojäsenvaltioperiaatteeseen, jonka mu-kaan terveydenhuollon tarjoajaan sovelletaan sen jäsenvaltion lakia, johon toimija on sijoit-tautunut.

Toimijan määritelmä

Valvira toteaa, että ehdotetun lain 3 §:n mukaisen toimijan määritelmän sitominen tervey-denhuollon osalta potilasdirektiivin 3 artiklan g-alakohdan mukaiseen terveydenhuollon tarjo-ajaan aiheuttaa kansallisesti tulkintatilanteita ja on epäselvää, mitkä tahot luetaan kyseisen määritelmän alaan.

Potilasdirektiivin mukaan terveydenhuollon tarjoajalla tarkoitetaan luonnollista henkilöä tai oi-keushenkilöä tai muuta kokonaisuutta, joka tarjoaa laillisesti terveydenhuoltoa jonkin jäsen-valtion alueella. Kansallisesti terveyspalveluita tuottavista tahoista (julkinen ja yksityinen pal-veluntuottaja) säädetään keskitetysti 1.1.2024 voimaan tulevassa sosiaali- ja terveydenhuol-lon valvonnasta annetussa laissa (741/2023, valvontalaki). On tärkeää huomioida, että val-vontalaissa erotetaan palvelunjärjestäjät, joilla on lakiin perustuva velvollisuus huolehtia asi-akkaiden ja potilaiden lakisääteisten palveluiden järjestämisestä ja saatavuudesta, sekä pal-veluja tosiasiallisesti tuottajat palveluntuottajat, jotka tulee rekisteröidä mainitun lain nojalla perustettavaan valtakunnalliseen rekisteriin.

Kyberturvallisuuslain perusteella on epäselvää, tarkoitetaanko siinä viitatulla terveydenhuol-lon tarjoajalla kansallisesti terveyspalveluiden järjestäjää vai tämän palveluntuottajaan, jotka voivat eri tahoja (esimerkiksi Kansaneläkelaitos on palvelunjärjestäjä, jonka korkeakoulu-opiskelijoiden

terveydenhuollon palveluita tuottaa Ylioppilaiden terveydenhoitosäätiö). Valvira ehdottaa kyberturvallisuuslakia täsmennettäväksi terveydenhuollon tarjoajan kansallisen määrittelyn osalta.

Valvira toteaa, että toimijan määritelmässä tai sen yksityiskohtaisissa perusteluissa on syytä huomioida myös terveyspalvelujen erilaiset tuottamismuodot. Käytännössä terveyspalveluja tuottava taho voivat siirtää palvelujen tosiasiallista tuottamista ostopalveluntuottajalle tai tä-män alihankkijoille. On tyypillistä, että esimerkiksi julkiseen järjestämisvastuuseen kuuluvaa palvelutoimintaa pilkotaan pienempiin kokonaisuuksiin, joita hankitaan yksityisiltä ostopalve-luntuottajilta erilaisilla alihankintaketjuilla. Edellä viitattu valvontalaki mahdollistaa niin sanot-tujen kuoriorganisaatioiden toiminnan, jossa palveluista vastaavalla palveluntuottajalla ei ole lainkaan omaa henkilöstöä. Palveluntuottaja voi myös hankkia omaa palvelussuhteista henki-löstöään täydentävää työvoimaa vuokraamalla sitä toiselta palveluntuottajalta. Vuokratyöti-lanteissa henkilöstö luetaan sitä tilaavan palveluntuottajan henkilöstömäärään, vaikka juridi-sesti vuokratyöntekijä ei ole palveluntuottajan palveluksessa.

Ehdotetun kyberturvallisuuslain mukaisen keskisuuren toimijan määrittelyssä olisi syytä täs-mentää esimerkiksi pykälien yksityiskohtaisissa perusteluissa, ketkä kaikki luetaan toimijan henkilöstömäärään (vähintään 50 työntekijää).

Riskienhallintavelvoitetta koskevat huomiot

-

Raportointivelvoitetta koskevat huomiot

-

Valvontaa koskevat huomiot

Poikkeamailmoitusten kansallinen koordinointi

Ehdotuksesta jää epäselväksi, tuleeko valvontaviranomaisen järjestää vuorokauden ympäri (24/7) jatkuva päivystys oman toimialansa merkittävien poikkeamien vastaanottoa ja käsittelyä varten, vai kuuluuko tällainen virka-ajan ulkopuolella tapahtuva päivystysvelvoite keskitetysti Kyberturvallisuuskeskuksen vastuulle. Valvira kannattaa kiireellisten, virka-ajan ulkopuolella tapahtuneiden merkittävien poikkeamailmoitusten keskittämistä Kyberturvallisuuskeskukseen, jolla on paras valmius ja substanssiasiantuntemus erityisesti ensivaiheen reagoinnille häiriötilanteissa ja kyberturvallisuutta turvaaville toimenpiteille ja ohjeistuksille. Kiireellisten tapausten lisäksi NIS2-direktiin toimeenpanossa tulee huolehtia siitä, että lakiin kirjattavat prosessit ovat selkeitä sen suhteen, mikä tai mitkä tahot koordinoivat lain mukaista viranomaistoimintaa kokonaisuudessa kansallisesti siten, ettei synny päällekkäisiä tehtäviä tai tilanteita, joissa samaa asiaa käsittelevät useat viranomaiset.

Seuraamusmaksua koskevat huomiot

-

CSIRT-yksikön tehtäviä koskevat huomiot

-

Tiedonhallintalakia ja täytäntöönpanoa julkishallinnossa koskevat huomiot

-

Verkkotunnusvälittäjiä koskevat huomiot

-

Kumottavaksi ehdotettuja säännöksiä koskevat huomiot

-

Vaikutustenarviointia koskevat huomiot

Uusien tehtävien vaatimat resurssit ja kyberturvallisuuden asiantuntemuksen varmistaminen

NIS1-valvontaan Valvirassa ei ole erillistä henkilöresurssia. NIS2-direktiivi laajentaa NIS1-direktiin mukaista valvontaa ja tuo hyvin merkittävästi lisää viranomaistehtäviä Valviralle. Työmäärän kannalta merkittävä muutos on keskeisiin toimijoihin kohdistettavan jälkikäteisvalvonnan lisäksi etukäteisvalvonta. Terveydenhuollon toiminta on laajaa Suomessa. Pelkästään yksityisiä terveydenhuollon keskeisiä toimijoita, joilla on vähintään 50 työntekijää, arvioidaan olevan tällä hetkellä noin 150 kpl. Yksityisten palveluntuottajien määrä on edelleen kasvussa. Lisäksi valvonnan kohteena ovat julkiset terveydenhuollon palveluntuottajat.

Valvira toteaa, että NIS2-direktiivin kansallisessa toimeenpanossa tulee huolehtia riittävistä Valviran omista resursseista ja kyberturvallisuuden asiantuntemuksen saatavuuden varmistamisesta. Direktiivin täytäntöönpano tulee aiheuttamaan esityksessä todetuin tavoin puutetta kansallisista kyberturvallisuuden osaajista ja hankaloittaa rekrytointeja virastoissa. Valvira näkee erittäin tärkeäksi, että valmistelussa varmistetaan virastokohtaisten lisäresurssien lisäksi kyberturvallisuuden asiantuntemuksen saamisesta ja asiantuntijoiden hyödyntämisestä Kyberturvallisuuskeskuksen kautta keskitetysti.

NIS2- voimaantulon jälkeen 19.10.2024 Valviralla pitäisi olla valmius vähintään kymmeniin vuosittaisiin fyysisiin, palveluntuottajan tiloissa tapahtuviin NIS2-tarkastuksiin. Ehdotuksen mukaan tarkastuksen suorittajalla on oltava tarkastuksen laatuun ja laajuuteen nähden riittävä koulutus ja kokemus. Ehdotettu valvontatehtävä sitoo usean virkamiehen työpanosta merkittävästi. Valviran lisäresurssoinnissa on huomioitava tarkastusta tekevien henkilöiden määrän lisäksi valvonta- ja tarkastustoiminnassa vaadittavan erityisosaamisen hankkimisen ja sektorialakohtaisen kouluttautumisen tarve.

NIS2-häiritilanteiden ilmoituskäytäntö muuttuu kolmivaiheiseksi, joka vastaa pääpiirteissään lääkinnällisten laitteiden ilmoituskäytäntöä ja ilmoitusten määräaikoja. Ehdotuksen mukaan Valviralla tulee olla valmius häiriöilmoitusten nykyistä nopeampaan käsittelyyn. Vaikka ehdotus mahdollistaa valvontaviranomaisen toiminnan priorisointia, esimerkiksi valvovan viranomaisen on vastattava poikkeamailmoituksen tehneelle taholle viivytyksettä (16 §). Ilmoitusmenettelystä on lisäksi ohjeistettava ja koulutettava toimijoita.

Kyberturvallisuuslaissa säädettäisiin viranomaisen valvontakeinoina turvallisuusauditoinnin tekemiseen velvoittamisesta, huomautusten ja varoituksen antamisesta, luvanvaraisen toiminnan rajoittamisesta tai luvan peruuttamisesta ja johdon toimen rajoittamisesta sekä näiden velvoitteiden tehostamisesta uhkasakolla. Ehdotettuun sääntelyyn sisältyy poikkeuksellinen oikaisuvaatimuksen tekeminen valvontapäätöksistä hallinnon itseoikaisukeinona ennen varsinaista valitusoikeuden käyttämistä (36 §). Valvira toteaa, että oikaisuvaatimusten käsittely on huomioitava toiminnan resurssoinnissa.

Valvira toteaa, että terveydenhuoltosektorin kyberturvallisuuden varmistaminen (erityisesti julkisessa terveydenhuollossa) on erittäin merkittävässä roolissa kansallisessa kyberturvallisuusuhkien varautumisessa ja epäkohtien käsittelyssä. Pääministeri Petteri Orpon hallituksen ohjelmassa 20.6.2023 on nostettu tavoitteeksi useassa kohtaa kyberturvallisuusuhkiin varautuminen ja yhteistyön parantaminen, muun muassa sosiaali- ja terveyspalveluiden tietojärjestelmien kyberturvallisuuden vahvistaminen.

Ehdotettu Valviran valvontatehtävä edellyttää hyvin spesifiä kyberturvallisuuden osaamista, jota Valviralla ei ole tällä hetkellä. Uusien rekrytointien lisäksi NIS2-tehtävät edellyttävät jatkuvaa asiantuntijoiden kouluttautumista ja alan seuraamista. Uusien tehtävien tärkeyden lisäksi pysyvien lisäresurssitarpeiden suuruutta arvioitaessa on huomioitava miten Valvira turvaa virastoon kertyvän terveydenhuollon kyberturvallisuuden asiantuntemuksen säilymisen ja jatkumisen esimerkiksi henkilöstövaihdostilanteissa, kun on ennakoitavissa, että samoista asiantuntijoista kilpailevat useat viranomaiset ja tahot. Riittävät henkilöstöresurssit turvaavat myös asiantuntijoiden veto- ja pitovoimaa virastossa. Valvira ehdottaa edellä todetun perusteella, että esityksessä varattujen kahden henkilötyövuoden (2 htv) sijaan virastolle varattaisiin NIS2-direktiivin uusien tehtävien suorittamiseksi vähintään kolme henkilötyövuotta (3 htv) sekä mahdollisuutta arvioida henkilöstöresurssitarvetta direktiivin voimaantulon jälkeen toiminnan vakiinnuttua.

Ehdotuksen mukaan Valviran tulisi ylläpitää toimijaluetteloa lain mukaisista toimijoista (43 §). Luettelon toteuttamista ja ylläpitoa varten Valviralle on ehdotettu kertaluonteisina korvauksi-na tietojärjestelmäinvestointeihin noin 0,15 M€ ja 10.000–20.000 euroa vuosittain 2025 alkaen, jotka on arvioitu tässä vaiheessa riittäviksi. Valvira toteaa, että NIS2-toimijaluettelon ylläpitämistä varten varattavia vuosittaisia korvauksia ja niiden tasoa tulee voida arvioida jatkossa ja tarvittaessa tehdä tasokorjauksia.

Muut huomiot ja avoin palaute esityksestä

Asiakastietolakiin ehdotetut muutokset

Valvira ei kannata kyberturvallisuuslain säätämisen yhteydessä sosiaali- ja terveydenhuollon asiakastietojen käsittelystä annettuun lakiin (703/2023, voimassa 1.1.2024 alkaen, asiakastietolaki) ehdotettuja muutoksia, jotka eriyttäisivät sosiaalihuollon ja terveydenhuollon palvelunantajan velvollisuuksia ja asettaisi toimijoille erilaisia vaatimuksia. Asiakastietolain 90 §:n 3 momenttiin ehdotettu teknillisluonteinen ja päällekkäisyyksien karsimiseksi tähtäävä uusi viittaus kyberturvallisuuslakiin tosiasiallisesti kaventaisi nykyisten palveluntuottajien yleiseen etuun perustuvia ilmoitusvelvollisuuksia häiriötilanteissa siten, että ilmoitusvelvollisuus koskisi jatkossa vain suurempia terveydenhuollon palvelunantajia.

Nykyisen asiakastietolain 90 §:n 3 momentin mukaan jos 1 ja 2 momentissa tarkoitetusta tietoturvallisuuteen liittyvästä poikkeamasta tai häiriöstä ilmoittaminen on yleisen edun mukaista, Valvira voi velvoittaa muun muassa palvelunantajan tiedottamaan yleisölle asiasta taikka kuultuaan ilmoitusvelvollista tiedottaa asiasta itse. Asiakastietolain mukainen ilmoitusvelvollisuus koskee kaikkia lain soveltamisalaan kuuluvia yksityisiä ja julkisia, isoja ja hyvinkin pieniä, käytännössä myös yksityisenä elinkeinonharjoittajana toimivia palvelunantajia niiden koosta tai toiminnan laajuudesta riippumatta.

Lakiehdotuksen mukaan edellä olevaa asiakastietolain 3 momenttia ehdotetaan muutettavaksi siten, että palvelunantajan sijaan sääntely koskisi vain sosiaalihuollon palvelunantajia, koska terveydenhuollon palvelunantajien velvoitteista säädettäisiin jatkossa kyberturvallisuuslaissa.

Ehdotetussa kyberturvallisuuslaissa tarkoitettuja toimijoita olisivat lähtökohtaisesti vain keskisuuret toimijat tai sitä suuremmat toimijat (yli 50 työntekijää tai tase yli 10 milj. euroa). Valvira toteaa, että kyberturvallisuuslain mukaisen toimijan määritelmä on merkittävästi suppeampi kuin asiakastietolain mukainen (terveydenhuollon) palvelunantajan määritelmä. Vaikka asiakastietolain 90 §:n 3 momentin mukainen ilmoitusvelvollisuus ja Valviran toimivalta tiedottaa itse merkittävistä poikkeamista vastaa sisällöllisesti ehdotetun kyberturvallisuuslain 14 §:n 3 momentin mukaista ilmoitusta, koskee jälkimmäinen säännös vain osaa asiakastietolain mukaisia palvelunantajia.

Koska NIS2-direktiivi asettaa vain minimivaatimukset unionin tason harmonisoinnille kyberturvallisuuden riskienhallinnassa, Valvira katsoo, että on perusteltua säilyttää kansallisesti laajemmat palvelunantajien ilmoitusvelvollisuutta koskevat vaatimukset asiakastietolaissa. Valvira ehdottaa, että asiakastietolain 90 §:n 3 momenttia ei muutettaisi NIS2-toimeenpanossa ehdotetulla tavalla.

Henriksson Markus
Valvira

Malava Arttu
Sosiaali- ja terveysalan lupa- ja valvontavirasto Valvira - Sosiaali- ja terveysalan lupa- ja valvontavirasto (Valvira)