Lääkealan turvallisuus- ja kehittämiskeskus Fimea

Lausunto

28.11.2023 FIMEA/2023/005644

Asia: VN/18157/2023

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

Lausunnonantajan lausunto

Yleiset huomiot NIS2-direktiivin tavoitteista ja tarkoituksesta

Kyberturvallisuusdirektiivin edellyttämä sääntely on Fimean valvonnassa olevan toiminnan näkökulmasta erittäin toivottua ja se ohjaa hyvin toimijoita kehittämään kyberturvallisuuttaan sekä velvoittaa riskienhallintatoimiin.

Soveltamisalaa koskevat huomiot

Esitykseen sisältyvän kyberturvallisuuden riskienhallinnasta annetun lain 1 §:n mukaan laissa säädettäisiin muun muassa yhteiskunnan toiminnan kannalta kriittisten toimijoiden kyberturvallisuuden riskienhallinta- ja raportointivelvoitteista sekä viranomaisten yhteistyöstä kybertuvallisuuspoikkeamien ja -riskien hallitsemiseksi. Lain 3 §:ssä säädettäisiin lain soveltamisalaan kuuluvista toimijoista. Kyseisen säännöksen mukaan toimijalla tarkoitettaisiin oikeushenkilöä tai luonnollista henkilöä, joka harjoittaa liitteessä I tai II tarkoitettua toimintaa tai on liitteessä I tai II tarkoitettua toimijatyppiä ja täyttää tai ylittää keksisuuren toimijan määritelmän. Säännöksen 2 momentin e kohdan mukaan toimijalla tarkoitettaisiin myös oikeushenkilöä tai luonnollista henkilöä, joka on CER-direktiivin nojalla määritelty kriittinen toimija. Lisäksi säännöksen 3 momentin nojalla valtioneuvoston asetuksella säädettäisiin lain soveltamisesta eräisiin toimijoihin.

Lakiehdotuksen liitteen I kohdassa 13 luetteloitaisiin terveysalan toimijat, joihin lakia sovellettaisiin. Esityksen perusteella terveysalan toimijoiden määrä on merkittävästi lisääntynyt verrattuna NIS1 direktiivin soveltamisalaan, johon kuuluivat ainoastaan terveydenhuollon tarjoajat. Lakiluonnoksen mukaan lakia sovellettaisiin terveydenhuollon toimijoiden lisäksi liitteen I 13 kohdan c alakohdan mukaan myös ihmiselle tarkoitettuja lääkkeitä koskevista yhteisön säännöistä annetun Euroopan parlamentin ja neuvoston direktiivin 2001/83/EY 1 artiklan 2 alakohdassa määriteltyjen lääkkeiden tutkimusta ja kehitystä harjoittaviin toimijoihin ja d alakohdan mukaan NACE Rev. 2-luokituksen C jakson kaksinumerotasossa 21 tarkoitettua lääkeaineiden ja lääkkeiden valmistusta harjoittaviin toimijoihin sekä e alakohdan mukaan Euroopan lääkeviraston roolin vahvistamisesta

kriisivalmiudessa ja -hallinnassa lääkkeiden ja lääkinnällisten laitteiden osalta annetun Euroopan parlamentin ja neuvoston asetuksen (EU) 2022/123 22 artiklassa tarkoitettuihin vakavan kansanterveysuhan aikana kriittisiksi katsottuja lääkinnällisiä laitteita (kansanterveysuhan aikana kriittisten lääkinnällisten laitteiden luettelo) valmistaviin toimijoihin.

Esitysluonnoksen Nykytila ja sen arviointi -kohdan (kohta 3) alakohdassa 3.5 on käsitelty vain hyvin yleisellä tasolla terveydenhuoltoalaa ja kerrottu muun muassa NIS2-direktiivin laajemmasta soveltamisalasta verrattuna NIS1 direktiiviin. Myöskään kyberturvallisuuden riskienhallinnasta annettavaa lakia koskevissa säännöskohtaisissa perusteluissa (kohta 7.1) ei ole ehdotuksen 1 ja 3 §:n kohdalla selostettu yksityiskohtaisesti tai edes esimerkinomaisesti, mihin kaikkiin toimijoihin säädöksen on tarkoitettu soveltuvan.

Lain säännösten ja esityksen perustelujen perusteella on vaikea saada selvyyttä, mihin yksittäisiin terveysalan toimijoihin sääntely kohdistuisi. Fimean toimialaan kuuluvista terveysalan toimijoista selkeimmin on määritelty lääkeaineiden ja lääkkeiden valmistusta harjoittavat toimijat sekä kriittisiä lääkinnällisiä laitteita valmistavat toimijat. Soveltamisalaa koskevan sääntely on kuitenkin kokonaisuutena sen vaikeaselkoisuuden, toimijoiden täsmentymättömyyden sekä niiden määrittelyyn liittyvän harkinnan vuoksi erittäin ongelmallinen paitsi toimijoiden myös valvovien viranomaisten kannalta. Soveltamisalan selkeydellä on suora vaikutus yhtäältä siihen, että toimijat ymmärtävät velvoitteensa ja noudattavat niitä ja toisaalta siihen, kuinka kattavasti valvova viranomainen voi täyttää sille kuuluvat valvontavelvoitteet. Kysymys on myös toimijoiden oikeusturvasta ja toimijoiden tasapuolisesta kohtelusta ottaen erityisesti huomioon valvoville viranomaiselle annettavat toimivaltuudet asettaa velvoitteiden rikkomisesta johtuvia seuraamuksia.

Soveltamisalan epäselvyys heikentää NIS2-direktiivin toimeenpanon, mikä voi aiheuttaa myös Suomeen EU:n jäsenvaltiona kohdistuvia toimenpiteitä, mikäli sen katsotaan laiminlyöneen velvoitteitaan direktiivin toimeenpanossa.

Fimean näkemyksen mukaan terveystoimialan soveltamisala jää hallituksen esityksessä niin epäselväksi, että se vaatii kokonaisuudessaan tarkentamista, jotta lakia kyberturvallisuuden riskienhallinnasta olisi mahdollista soveltaa ja soveltamista valvoa tarkoitetulla tavalla ja tarkoitetussa laajuudessa.

Edellä mainitun vuoksi Fimea ei esityksen perusteella pysty täysin hahmottamaan omia velvoitteidensa laajuutta valvovana viranomaisena eikä siten myöskään arvioimaan täysin esityksen vaikutuksia toimintaansa.

Soveltamisalan lisäksi esityksessä tulee vielä arvioida ja tarkentaa sitä, mitkä terveystoimialan toimijat kuuluvat minkäkin valvovan viranomaisen (Valvira vai Fimea) valvontavaltaan ja mahdollisen jaetun valvontavastuun osalta toimivallan selkeä rajaus.

Edellä esitetyn lisäksi Fimea esittää seuraavia sektorikohtaisia huomioita kyberturvallisuuden riskienhallinnasta annetun lain soveltamisalasta:

Euroopan parlamentin ja neuvoston direktiivin 2011/24/EU 3 artiklan g alakohdassa määritellyt terveydenhuollon tarjoajat on jätetty nyt lausuttavana olevassa hallituksen esityksessä tarkemmin määrittelemättä laajentuneen sääntelyn toimialaan mahdollisesti kuuluvien, Fimean valvonnassa olevien toimijoiden osalta. Hallituksen esityksessä todetaan muun muassa, että sosiaali- ja terveydenhuollon palveluntarjoajat ovat olleet NIS1 -direktiivin piirissä eikä NIS2 -direktiivi tuo merkittäviä muutoksia soveltamisalaan näiden toimijatyyppien osalta (s. 56, Terveyssektori). Yksityisten sosiaali- ja terveydenhuollon toimijoiden todetaan kuuluvan kyberturvallisuuden riskienhallinnasta annettavan lain soveltamisalaan ja lisäksi todetaan, että valvovana viranomaisena on toiminut NIS1 -velvoitteiden osalta Valvira. Hallituksen esityksessä todetaan uusina NIS2 -direktiivin soveltamisalaan tulevina toimijoina EU:n vertailulaboratoriot (eivät Fimean valvonnassa) sekä Fimean valvonnassa olevat lääkkeiden tutkimus- ja kehitystoiminta sekä lääkkeiden, lääkeaineiden tai lääkinnällisten laitteiden valmistus. Terveyssektorilla NIS2 - direktiivin laajenevan soveltamisalan todetaan tuovan velvoitteiden piiriin uusia toimijatyyppejä ja näin kasvattavan valvottavien toimijoiden määriä.

Hallituksen esityksessä (s. 25, 3.5.1 Terveydenhuollon tarjoajat) viitataan muun muassa sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annettuun lakiin 784/2021 (vrt. 703/2023 alkaen 1.1.2024) sekä todetaan lain 7 §:n velvoittavan palvelunantajan liittymään valtakunnallisten tietojärjestelmäpalveluiden käyttäjäksi (Kanta -palvelut). Sääntelyn todetaan koskevan julkisia terveydenhuollon tarjoajia sekä yksityisiä toimijoita, mikä niillä on käytössään asiakas- ja potilastietojen käsittelyyn tarkoitettu tietojärjestelmä. Tällaiseksi tietojärjestelmäksi katsotaan yleisesti lääkemääräysten toimittamisessa tarvittavat apteekkitietojärjestelmät. Apteekkitoimijoiden ja lääkkeiden toimittamisessa apteekkien käyttämien tietojärjestelmien asema soveltamisalan määrittelyissä tai valvontavastuissa ei kuitenkaan Fimean näkemyksen mukaan hallituksen esityksestä selvästi ilmene. Fimea valvoo lääkelain nojalla yleisesti apteekkitoimintaa, mistä johtuen Fimean valvontarooli ja toisaalta Valviran tietojärjestelmävalvontaan liittyvä rooli olisi tarpeen nyt valmisteltavana olevassa laissa ja sen esitöissä selkeyttää.

On lisäksi hyvä ottaa huomioon, että Fimea valvoo myös laitosten lääkehuollosta vastaavia sairaala-apteekkeja ja lääkekeskuksia. Puolustusvoimien lääkehuoltoa varten on lisäksi Sotilasapteekki, jota myös Fimea osaltaan valvoo.

Veripalvelutoiminta, josta vastaa Suomessa tällä hetkellä ainoana toimiluvallisena toimijana Suomen Punaisen Ristin Veripalvelu, on Fimean valvonnassa. Fimean valvonnassa ovat myös hoitokäyttöön tarkoitettuja kudos- ja solusiirteitä käsittelevät kudoslaitokset sekä elinsiirteet niiden laadun, turvallisuuden ja jäljitettävyyden osalta. Elinsiirrot kuten muutkaan hoitotoimenpiteet edellä mainittuja siirteitä käyttäen eivät ole Fimean valvonnassa. Elinsiirtotoiminta on Suomessa täysin keskittynyttä ja toimintaa koordinoi HUS Elinsiirtotoimisto. Myös näiden toimijoiden kuuluminen nyt

valmisteltavana olevan lain soveltamisalaan tulisi arvioida samoin kuin selkeyttää niihin liittyvät Fimean valvontavastuut.

Lääkkeiden tutkimusta ja kehitystä harjoittavien toimijoiden osalta voidaan todeta, että Fimea valvoo lääkkeiden prekliinistä tutkimusta sekä ei-kliinistä (kemikaalit ym.) tutkimusta tekeviä laboratorioita ja niissä noudatettavaa hyvää laboratoriokäytäntöä (GLP, Good Laboratory Practice). Fimea valvoo myös kliinisiä lääketutkimuksia ja niissä noudatettavaa hyvää kliinistä tutkimustapaa (GCP, Good Clinical Practice). Kliinisten lääketutkimusten valvonnan osalta ”toimijan” määrittely vaatii Fimean näkemyksen mukaan selkeyttämistä. Kliinisiä lääketutkimuksia koskevan asetuksen (EU) N:o 536/2014 artiklan 2 mukaan esimerkiksi toimeksiantaja määritellään seuraavasti (kohta 14): toimeksiantajalla tarkoitetaan henkilöä, yritystä, laitosta tai organisaatiota, joka vastaa kliinisen lääketutkimuksen aloittamisesta, hallinnoimisesta ja rahoituksen järjestämisestä. Käytännössä toimeksiantajia ovat lääkeyritykset, tutkijaryhmät, sairaalat tai yksittäiset akateemiset tutkijat. Fimea toivoo, että NIS2-direktiivin mahdollistamat delegoidut säädökset toisivat osaltaan tulkinta-apua tältä osin.

NIS2-direktiivin liitteen I terveystoimialan toimijoista puuttuvat tukkukaupan harjoittamista koskevien lupien haltijat eli lääketukkukaupat (direktiivi 2001/83/EY, 79 artikla). Lääketukkukaupat sisältyvät kuitenkin CER-direktiivin (EU) 2022/2557 liitteen mukaisesti kyseisen direktiivin soveltamisalaan. Fimean näkemyksen mukaan lääketukkukaupat tulisi tunnistaa selvyyden vuoksi myös kansallisessa lainsäädännössä kyberturvallisuuden riskienhallinnassa kriittisiksi toimijoiksi eikä ainoastaan viitata CER ja NIS2-direktiivien yhtenäiseen soveltamisalaan.

Lääkinnällisten laitteiden valmistajiin voidaan kohdistaa riskiperusteista ja sääntelyn edellyttämää etukäteis- ja jälkikäteisvalvontaa, kun vastuut ja toimivaltuudet ovat selkeästi kuvattu ja valvottavat toimijat tunnistettu. Fimean arvioi, että Hyvinvointialueiden kautta voitaisiin saada ajantasainen tieto heidän tunnistamistansa keskeisistä ja tärkeistä toimijoista, joihin valvova viranomainen voi toteuttaa eri sääntelyissä edellytetyt toimet (EU asetus 2022/123, CER-direktiivi ja NIS2-direktiivi, laki 719/2021 sekä laki 741/2023). Lakiehdotukseen ei kuitenkaan sisälly mallia, jolla Hyvinvointialueet velvoitettaisiin jakamaan tiedot tunnistamistaan keskeisistä ja tärkeistä toimijoista kyberturvallisuuden valvonnan edellyttämällä tavalla ja siltä osin Fimealla ei ole selkeää keinoa kerätä tietoa terveydenhuollon kannalta kriittisistä toimijoista näiden toimijoiden valvonnan järjestämiseksi. Lisäksi HE:n liitteessä II kohditien 9 ja 10 määritelmä kattaa myös lääkinnällisiä laitteita yksilölliseen käyttöön valmistavat valmistajat, joka laajentaa Fimean näkemyksen mukaan valvottavien toimijoiden määrän direktiivin tarkoittamaa laajemmaksi.

Soveltamisalasta olisi tärkeää tehdä vertailu muihin EU-maihin tai ainakin muihin Pohjoismaihin sen arvioimiseksi, että onko soveltamisala määritelty samoin, ja koskevatko uudet velvoitteet ja niistä aiheutuvat kustannukset tasapuolisesti saman toimialan toimijoita EU-markkinoilla. Kyberturvallisuuden sekä riskienhallintatoimien kannalta on tärkeää, että soveltamisala on tarkkaan harkittu ja kattaa kriittiset toimijat, mutta toisaalta kustannusvaikutusten takia on tärkeää, että soveltamisalaa ei uloteta sellaisiin toimijoihin, joiden kohdalla NIS2-direktiivin tarkoittama säätely on suhteettoman raskas saatavaan hyötyyn nähden.

Riskienhallintavelvoitetta koskevat huomiot

Kyberturvallisuuden riskienhallinta tuo velvoitteita myös Fimean tietoturvallisuuden hallintamalliin ja käytäntöihin, minä vuoksi Fimean on päivitettävä ja kehitettävä tietoturvallisuuden hallintamallia ja käytäntöjä. Fimea käyttää hallintamallin ja käytäntöjen kehittämiseen palveluntarjoajaa ja arvio sen kustannuksien olevan noin 100 000€. Fimea on siirtymässä Valtorin palveluiden piiriin ja viraston tietoturvallisuus perustuu jatkossa pitkälti Valtorin tuottamiin ratkaisuihin. Fimea esittää, että Valtorin tarjoamien palveluiden osalta Valtori huolehtii siitä, että sen tarjoamat ratkaisut noudattavat NIS2 – direktiiviä. Fimea esittää, että mahdolliset muutokset hoidetaan ja rahoitetaan keskitetysti.

Kyberturvallisuuden riskienhallinnasta annettu esitys sisältää vaatimuksia kyberturvallisuuden riskienhallinnasta siten, että se toimeen panee NIS2-direktiivin vähimmäisvelvoitteet. NIS2-direktiivin 21 artikla sisältää luettelon toimenpiteistä, jotka on otettava käyttöön ja joiden takia Fimean tietohallinnan kyberturvallisuusriskien hallintatoimenpiteitä koskevat tehtävät lisääntyvät. Kyseiset uudet riskienhallinnan velvoitteet lisäävät viraston kustannuksia.

Vastaavalla tavalla uudet riskienhallinnan velvoitteet lisäävät kaikkien soveltamisalaan kuuluvien toimijoiden kustannuksia ja siksi olisi tärkeää määritellä soveltamisala siten, että uudet velvoitteet koskevat toimijoita vain kun se on perusteltua. On myös tärkeää tehdä vertailu muihin EU-maihin tai ainakin muihin Pohjoismaihin sen arvioimiseksi, että onko soveltamisala määritelty samoin ja koskeeko uudet riskienhallintavelvoitteet ja niiden kustannukset tasapuolisesti samassa markkinassa kilpailevia toimijoita. Markkinoiden toimivuuden kannalta on oleellista, että ei aiheuteta markkinamuutoksia, jotka heijastuvat lääkkeiden tai laitteiden saatavuuteen.

Raportointivelvoitetta koskevat huomiot

HE:ssä todetaan, että Traficomin Kyberturvallisuuskeskus toimii tietoturvaloukkauksiin reagoivana ja niitä tutkivana CSIRT-yksikkönä. Hallituksen esityksen mukaan Fimealle tulisi uusia velvollisuuksia tietoturvapoikkeamien raportoinnista CSIRT-yksikölle siten, että tietoturvapoikkeamista tulisi tehdä ensi-ilmoitus 24 tunnin sisällä havainnoimisesta, ja jatkoilmoitus 72 tunnin kuluessa ja loppuraportti kuukauden sisällä. Fimean tietohallinnolla ei ole päivystysvelvollisuutta, jolta osin 24 tunnin vaade on vaikeasti toteutettava ja vaatii muutoksia toimintaan.

Valvontaa koskevat huomiot

Esitysluonnoksessa on käsitelty toimijoihin kohdistuvien velvoitteiden valvonnan järjestämisvaihtoehtoina sektorikohtaista valvontaa ja keskitettyä valvontaa. Esityksessä on todettu, että NIS2-sektoreilla on olemassa olevia valvontaviranomaisia, jotka valvovat niille sektorikohtaisessa lainsäädännössä määritettyjä kokonaisuuksia tai osa-alueita muun ohella turvallisuuden ja riskienhallinnan osalta. Esityksessä on päädytty esittämään sektorikohtaista valvontaa ja valintaa on perusteltu muun muassa sillä, ettei kyberturvallisuus ole valvottavan

toimijan muusta toiminnasta erillinen osa, vaan yhteiskunnan digitalisoituessa kyberturvallisuus hahmotetaan toiminnan kokonaisturvallisuuden osa-alueena. Sektorikohtaisesta valvontaa on perusteltu muun muassa sillä, että valvovat viranomaiset voisivat valvonnassa kiinnittää huomiota sektorikohtaisiin erityispiirteisiin. Myös toimijoiden näkökulmasta on pidetty selkeämpänä ja vähemmän hallinnollista taakkaa aiheuttavana ratkaisuna, ettei erilaisten riskien hallintaan tai toiminnan turvallisuuteen ja jatkuvuuteen liittyvien velvoitteiden valvontaa ja häiriöiden raportointia ole hajautettu useille viranomaisille, vaan toimijaa valvoisi lähtökohtaisesti yksi viranomainen toimintaan kohdistuvien turvallisuus- ja riskienhallintavelvoitteiden osalta.

Esityksen perusratkaisuna oleva kyberturvallisuuden riskienhallinnan sektorikohtainen valvonta ei Valviran ja Fimean ei toteudu esityksessä selkeästi määritellyllä tavalla ja esityksen mukaankin Fimean osuus täydentyy.

Fimean nykyiseen sektorikohtaiseen toimivaltaan perustuen Fimea valvoisi kyberturvallisuusdirektiivin (EU) 2022/2555 Terveys -toimialassa mainittuja lääkeaineiden ja lääkkeiden valmistusta harjoittavia toimijoita. Suomessa toimii 35 teollisen lääkevalmistuksen toimiluvan haltijaa, joiden toiminta poikkeaa toisistaan paljon valmistettavan lääkevalikoiman ja valmistusvolyymien osalta.

Lääkkeiden tutkimus- ja kehitystoiminnan osalta voi todeta, että Fimea valvoo prekliinistä / ei-kliinistä tutkimusta tekeviä laboratoriota (GLP), joita on Suomessa yhteensä viisi. Näistä neljällä on toimialassaan prekliiniset tutkimukset. Fimean valvoo kliinisiä lääketutkimuksia, mutta direktiivin toimijatyypin määrittely lääkkeiden tutkimusta ja kehitystä harjoittavista toimijoista edellyttää selkeyttämistä, jotta valvottavien toimijoiden lukumäärää voitaisiin arvioida.

Fimea valvoo ns. vakavan kansanterveysuhan aikana kriittisiksi katsottuja lääkinnällisiä laitteita valmistavia toimijoita. Suomessa toimii arviolta 30 tällaista toimijaa, jotka voitaisiin kriisitilannekohtaisesti katsoa kuuluvaksi soveltamisalaan. Näiden ns. vakavan kansanterveysuhan aikana kriittisiksi katsottujen lääkinnällisiä laitteita valmistavien toimijoiden lisäksi HE:n kohdassa 3 § kohdassa e) laajennetaan valvonta koskemaan CER-direktiivin nojalla kriittisiksi määriteltyjä toimijoita, joiden osalta määritelmää ei vielä ole olemassa. Fimean arvion mukaan CER-direktiivin nojalla kriittisiksi määriteltyjä toimijoita saattaisi olla joitakin kymmeniä tai jopa satoja. Fimean rekisterissä on tällä hetkellä noin 900 toimijaa ja rajausta kriittisiksi katsottuihin toimijoihin ei ole vielä määritelty. Kyberturvallisuuden riskienhallinnasta annettavan lain 25 §:n 1 momentin d kohdan mukaan Valvira olisi vakavan kansanterveysuhan aikana kriittisiksi katsottuja lääkinnällisiä laitteita valmistavia toimijoita NIS2-direktiivin mukaan valvova viranomainen. Muulloin kuin vakavan kansanterveysuhan aikana lääkinnällisten laiteita valmistavia toimijoita sen sijaan valvoisi Fimea. Valvontavastuu kybertuvallisuuden riskienhallinnasta seuraavien velvoitteiden noudattamisessa jakautuisi siis lääkinnällisiä laitteita valmistavien toimijoiden kohdalla Valviran ja Fimean kesken riippuen siitä, onko kysymyksessä vakava kansanterveyttä uhkaava tilanne vai ei. Kyseisen valvontavastuun jako ei ole millään tavalla perusteltu eikä mielekäs ja valvontaviranomaiseksi lääkinnällisiä laitteita valmistavien toimijoiden kohdalla tulisi kaikissa tilanteissa olla Fimea.

Edellä esitettyjen lisäksi laki kybertuvallisuuden riskienhallinnasta tulisi Fimean käsityksen mukaan koskemaan madollisesti myös eräitä muita toimijoita, joihin myös laissa tarkoitettu valvonta tulisi kohdistumaan. Fimean näkemyksen mukaan kyseisenkaltaisia toimijoita voisivat olla seuraavat:

Kyberturvallisuusdirektiivin liitteen I mukaisia mahdollisia terveydenhuollon tarjoajia tai kansallisesti määriteltyjä muita kriittisiä Fimean valvonnassa olevia toimijoita voisivat olla apteekit. Suomessa on noin 630 pääapteekkia sekä 190 sivuapteekkia. Avohuollon apteekkien lisäksi on otettava huomioon laitosten lääkehuolto, josta vastaavat nykyisellään Fimean valvonnassa olevat sairaala-apteekit (24) sekä lääkekeskukset. Puolustusvoimien lääkehuoltoa varten on lisäksi Sotilasapteekki.

Suomessa on yksi toimiluvallinen veripalvelutoimija, jolla on päätoimipisteen lisäksi 10 toimipistettä eri puolilla maata. Fimea valvoo myös kudoslaitoksia, joita on Suomessa noin 40 sekä elinsiirteiden laatua, turvallisuutta ja jäljitettävyyttä. Elinsiirteiden ja elinsiirtotoiminnan koordinaatiosta vastaa Suomessa keskitetysti HUS Elinsiirtotoimisto.

Suomessa on tällä hetkellä noin 100 Fimean valvonnassa olevaa lääketukkukauppatoimiluvan haltijaa, joista lääkkeiden jakelu ja laaja varastointi on keskittynyt käytännössä viidelle luvanhaltijalle. Muut kuin mainitut jakelijatukut harjoittavat tyypillisesti myös lääkkeiden maahantuontia, minkä takia niiden toiminnan jatkuvuus on olennaista lääkkeiden saatavuuden näkökulmasta.

Fimean näkemyksen mukaan kyberturvallisuuden riskienhallinnasta annetun lain täytäntöönpano terveystoimialalla tulisi vaatimaan paljon ohjausta ja neuvontaa. Valvontaa toteuttavilla viranomaisilla tulee olla ajantasainen tieto kyberturvallisuuden vaatimuksista ja hallintakeinoista ja kyseistä osaamista ei ole muun muassa Fimeassa. Sen vuoksi NIS2-direktiivin ja kyberturvallisuuden riskienhallinnasta annetussa laissa edellytetyn valvonnan järjestäminen edellyttää Fimeassa uudenlaista osaamista ja kouluttautumista, laatujärjestelmän ohjeistuksen täydentämistä, kriittisten toimijoiden kartoitusta ja nimeämistä sekä toimijoiden ohjausta ja neuvontaa niiden uusista vastuista ja velvoitteista. Fimea arvio, että tähän tarvitaan noin 700 k€:n rahoitusta sääntelyn täytäntöönpanovaiheessa vuosina 2024 - 2025. Valvontaan arvioidaan tarvittavan Fimean valvomien toimialojen osalta yhteensä minimissään viiden henkilötyövuoden (5 htv) asiantuntijaresurssit pysyvästi, jotta valvonta, raportointi sekä toimijoiden ohjaus voidaan hoitaa asianmukaisesti. Lisäksi Fimean joutuu kehittämään valvontaa tukevan tietojärjestelmän, jonka rahoitukseen arvioidaan tarvittavan n. 500 000 €. Kyseiset arviot perustuvat siihen, että edellä kuvatut Fimean valvonnassa tällä hetkellä olevat toimijat kuuluisivat kyberturvallisuuden riskienhallinnasta annettavan lain soveltamisalaan. Arviosta puuttuvat kuitenkin lääkkeiden tutkimusta ja kehitystä harjoittavat toimijat, koska tämän toimijatyypin mukaisten toimijoiden määrittely edellyttää Fimean tarkempia linjauksia lain soveltamisalasta. Kyberturvallisuuden valvontaa ei voida katsoa olevan toimijoille maksullista valtion maksuperustelain (150/1992) mukaisesti ja siksi NIS2-valvonnan tulee olla budjettirahoitteista.

Lain soveltamisalaa sekä siinä säädettyä valvontatoimivaltaa ja sen jakautumista eri viranomaisten (Fimea ja Valvira) kesken on välttämätöntä arvioida ja tarkentaa esityksen jatkokäsittelyssä ennen kuin valvonnasta ja sen toteuttamisesta sekä tarvittavista resursseista on mahdollista esittää edellä esitettyä tarkempia näkemyksiä.

Esitys lähtee siitä, että kyberturvallisuuden riskienhallinnasta annetussa laissa tarkoitettu valvontavastuu jakautuisi sektoriviranomaisille sen mukaisesti kuin ne muutenkin valvovat toimijoiden turvallisuus- ja riskienhallintavelvoitteiden toteutumista. Fimea katsoo, että näin myös tulee olla. Esityksessä on kuitenkin ristiriita valvontaa koskevan perusratkaisun (sektorikohtainen valvonta) ja valvontavastuuta (Valvira/Fimea) koskevien säännösten välillä. Fimea katsoo, ettei sen valvontatoimivaltaa ja velvoitteita ole riittävän selkeästi määritelty esityksessä. Riittämättömästi määritetyt velvollisuudet vaarantavat esityksen edellyttämän valvonnan toteutumisen.

Seuraamusmaksua koskevat huomiot

Kybertuvallisuuden riskienhallinnasta annetun lain 5 luvussa säädetystä seuraamusmaksulautakunnasta ja menettelystä seuraamusmaksujen määräämisessä tarvitaan ohjausta ja neuvontaa valvoville viranomaisille.

CSIRT-yksikön tehtäviä koskevat huomiot

Fimea esittää, että kansalliselle yhteyspisteelle Traficomin Kyberturvallisuuskeskuksen CSIRT-yksikölle tulisi laaja rooli tarjota kyberturvallisuuden asiantuntija-apua valvoville viranomaisille. Valvonnan tasalaatuisuuden ja kustannustehokkuuden kannalta kyberturvallisuuden osaamista ei ole järkevää rakentaa kaikilta osin jokaisen valvovan viranomaisen organisaatioon vaan asiantuntijatuen osalta keskitetty hybridimalli olisi kustannustehokkaampi ja nopeuttaisi lain täytäntöönpanoa.

Tiedonhallintalakia ja täytäntöönpanoa julkishallinnossa koskevat huomiot

-

Verkkotunnusvälittäjiä koskevat huomiot

-

Kumottavaksi ehdotettuja säännöksiä koskevat huomiot

-

Vaikutustenarviointia koskevat huomiot

Fimea katsoo, että sen osalta vaikutustenarviointi on tehty puutteellisesti ja vajavaisesti, koska HE:n kappaleessa 4.4 Vaikutukset viranomaisten toimintaan on lyhyesti todettu, että Fimean osuus täydentyy myöhemmin.

Fimea näkemyksen mukaan koko terveystoimialaa koskeva vaikutustenarviointi on yleisesti hyvin vajavainen ja puutteellinen. Esitys ei sisällä riittävän yksityiskohtaisia tietoja kyberturvallisuuden riskienhallinnasta annettavan lain soveltamisalaan kuuluvista terveysalan toimijoista eikä toimijoihin kohdistuvista vaikutuksista, kuten ei myöskään vaikutuksista valvoville viranomaisille, kuten Fimealle.

Epäselvyys edellä mainitun lain soveltamisalasta on vaikeuttanut terveystoimialan toimijoiden mahdollisuuksia esityksen perusteella tunnistaa, kuuluvatko ne lain soveltamisalaan, mikä on voinut vaikuttaa toimijoiden mahdollisuuksiin ja tarpeisiin lausua esityksestä. Sen vuoksi menossa olevalla lausuntokierroksella ei välttämättä ole mahdollista saada esityksen jatkovalmisteluun kaikkia tarpeellisia näkemyksiä, mikä osaltaan heikentää mahdollisuuksia kattavaan terveystoimialan vaikutusten arviointiin.

Muut huomiot ja avoin palaute esityksestä

Fimean näkemyksen mukaan kybertuvallisuuden riskienhallinnasta annetun lain soveltamisalan tarkempi määrittely terveystoimialalla olisi ehdottoman välttämätöntä, jotta toimijat ja valvovat viranomaiset tietäisivät velvollisuutensa, valvovat viranomaiset voisivat suorittaa valvontatehtäväänsä tehokkaasti ja tasalaatuisesti ja Suomi EU:n jäsenvaltiona täyttää velvoitteensa NIS2-direktiivin toimeenpanossa. Fimean näkemyksen mukaan esityksestä on tarpeen täydentää ja tarkentaa, jotta näihin tavoitteisiin päästään.

Peltoniemi Susanna
Lääkealan turvallisuus- ja kehittämiskeskus Fimea