Sosiaali- ja terveysalan lupa- ja valvontavirasto Valvira

Lausunto

15.09.2025 V/34260/2025

Asia: VN/27546/2023

Lausuntopyyntö luonnoksesta hallituksen esitykseksi eduskunnalle laeiksi turvallisuustutkintalain ja kyberturvallisuuslain 17 §:n muuttamisesta

Lausunnonantajan lausunto

Voitte kirjoittaa lausuntonne alla olevaan tekstikenttään

Turvallisuustutkintalakia ehdotetaan muutettavaksi siten, että se vastaisuudessa mahdollistaisi Onnettomuustutkintakeskukselle (Otkes) toimivallan suorittaa kyberturvallisuuteen kohdistuneiden erittäin vakavien kyberturvallisuuspoikkeamien turvallisuustutkintaa. Lakimuutos tulisi voimaan vuoden 2027 alusta, joten se ei koskisi enää Sosiaali- ja terveysalan lupa- ja valvontavirastoa (Valvira) vaan 1.1.2026 toimintansa aloittavaa Lupa- ja valvontavirastoa (LVV). Valviran nykyisiin, LVV:lle siirtyviin, tehtäviin kuuluu kyberturvallisuuden valvontaan liittyviä tehtäviä sosiaali- ja terveydenhuollossa.

Valvira kiinnittää huomiota ehdotetun turvallisuustutkintalain 1 a §:n määritelmään erittäin vakavasta kyberturvallisuuspoikkeamasta. Valvira kannattaa kyberturvallisuuspoikkeaman määritelmän sitomista mahdollisimman pitkälle kyberturvallisuuslain käsitteistöön selkeyden vuoksi. Viime kädessä kyseisen määritelmän tulkinta kuuluu Otkesille, joka päättää, milloin kyse on sen tutkintatoimivaltaan kuuluvasta erittäin vakavasta kyberturvallisuuspoikkeamasta. Käytännössä määritelmän tulkinnasta voi aiheutua myöhemmin mainittuja haasteita, joita joudutaan ratkomaan tapauskohtaisesti.

Väljästi laaditun 1 a §:n vakavan kyberturvallisuuspoikkeaman määritelmän takia lakiehdotuksen 16 a §:n ilmoitusvelvollisuuden realisoituminen voi aiheuttaa pulmatilanteita valvovassa viranomaisessa. Koska määritelmä on niin kattava/väljä, tulee valvovalla viranomaisella kuten LVV:lla olemaan haasteita luokitella sen saamia kyberturvallisuuslain mukaisia poikkeamailmoituksia erittäin vakaviksi. Näin ollen hallituksen esityksen perusteluissa taikka jopa lakitekstissä tulisi ottaa kantaa siihen, voiko valvontaviranomainen esimerkiksi tarvittaessa neuvotella salassapitosäännösten estämättä Otkesin kanssa yksittäisistä tapauksista ja siitä, että tulisiko sen tehdä ilmoitus Otkesille ehdotettavan 16 a §:n perusteella.

Valvira kiinnittää huomiota myös siihen, ettei lakiehdotuksen 16 a §:n mukaiselle ilmoitukselle ole säädetty aikamäärettä. Jotta tutkinta olisi mahdollisimman onnistunut, ilmoitus tulisi kaiketi tehdä mahdollisimman nopeasti? Tulisiko ilmoituksen tekemiselle säätää aikamääre, joka alkaisi ilmoittajan saatua tietää tapahtumasta?

Lisäksi Valvira haluaa nostaa esiin sen seikan, että valvovan viranomaisen ilmoittaessa 16 a §:n mukaisesti Otkesille erittäin vakavasta kyberturvallisuuspoikkeamasta käynnistyy käytännössä kaksi samaa asiaa arvioivaa tutkintaa. Oletettavasti kummatkin viranomaiset suorittavat valvonta- ja tutkintatehtäviään itsenäisesti ja toisistaan riippumattomasti, vaikka kyse on samasta tapahtumasta/toiminnasta. Lähtökohtaisesti asioiden samanaikainen käsittely on perusteltua, koska viranomaisilla on erilainen tehtävä, mutta käytännössä voi (tosin harvinaista kuitenkin) syntyä tilanne, jossa viranomaiset päätyvät eri ratkaisuihin.

Ehdotetussa 20 a §:ssä säädetty Otkesin tiedonsaantioikeus on laaja ja käsittää monia Valviran/LVV:n kyberturvallisuuden valvonta-asiassa hankittuja tai saatuja asiakirjoja. Pykälässä mainitut kyberturvallisuuslain 11–13 §:n mukaiset asiakirjat koskevat toimijan tekemiä ilmoituksia ja niiden jatko-osia/-raportteja, mutta 28 §:n 1 ja 2 momentissa tarkoitetut tiedot voivat koskea laajasti hyvin erilaisia LVV:n viran puolesta hankkimia tai laatimia asiakirjoja, kuten asiantuntijalausuntoja, tarkastuskertomuksia ja muita selvityksiä. Jotta LVV voi hoitaa omia kyberturvallisuuslain mukaisia valvontatehtäviään tehokkaasti, sen on saatava jatkossakin toimijoilta riittävät ja totuudenmukaiset selvitykset kyberturvallisuuspoikkeamista. LVV:n hankkimien tietojen mahdollinen luovuttaminen edelleen Otkesille voi vähentää toimijoiden selvityksenantohalukkuutta ja vaikeuttaa LVV:n omien tehtävien suorittamista. Lisäksi Valvira kiinnittää huomiota siihen, että Otkesin tutkinnan suorittamisen kannalta välttämättömien ja oikeuden tietojen luovuttaminen edellyttää tiivistä yhteistyötä viranomaisten välillä.

Lakiluonnoksen 28 §:ssä esitetään, että erittäin vakavan kyberturvallisuuspoikkeaman tutkintaselostuksen luonnoksesta voisi antaa lausuntoja. Valvira pitää tällaista lisäystä erittäin tärkeänä, koska näin Valvira pystyy antamaan oman panoksensa tutkintaselostukseen omaan valvontatoimivaltansa ja -kokemuksensa perusteella. Tällainen viranomaisyhteistyö on erittäin tärkeää myös siksi, että oletettavasti lähes jokainen erittäin vakava kyberturvallisuuspoikkeama on Otkesin tutkinnan kanssa samanaikaisesti Valviran/LVV:n kyberturvallisuuslain nojalla valvottava tapaus. Lausunnon antamisella on LVV:a hieman työllistävä vaikutus.

Lakiehdotuksen 39 §:n osalta Valvira ehdottaa, että pykälän 2 momentin yksityiskohtaisiin perusteluihin lisätään selkeyden vuoksi, että Otkesilla olisi oikeus luovuttaa mainitun momentin perusteella LVV:lle salassapitosäännösten estämättä erittäin vakavan kyberturvallisuuspoikkeaman tutkinnassa saatuja tietoja, jos se on välttämätöntä tärkeän yleisen edun turvaamiseksi. Yleistä etua olisi tässä yhteydessä arvioitava laajasti koskemaan LVV:n käsittelemiä merkittäviä kyberturvallisuuden poikkeamatilanteissa, joissa tilanteen korjaaminen tai uusien vahinkojen tai haittatapahtumien ennaltaehkäisy edellyttää toimijalta aktiivisia toimia ja/tai muutoksia nykyiseen toimintaansa. Salassa pidettävien tietojen luovuttamista Otkesilta LVV:lle perustelee erityisesti se, että vain LVV:lla on mahdollisuus aloittaa oma valvonta ja antaa valvonnassa toimijoita velvoittavia

seuraamuksia tilanteissa, joissa kyberturvallisuuslain mukaisia vaatimuksia on rikottu (esim. johdon toiminnan rajoittaminen, kyberturvallisuusauditoinnin teettäminen ja muut velvoittavat määräykset puutteiden korjaamiseksi sekä tarvittaessa niiden tehostaminen uhkasakolla). Otkesilla ei ole toimivaltaa antaa kyberturvallisuuslain mukaisia seuraamuksia ja jäädä valvonnallisesti esimerkiksi seuraamaan vakavan poikkeaman jälkeistä tilannetta ja puutteiden korjaamista. Valviran näkemyksen mukaan olisi kestämätön tilanne, jos Otkesilla olisi valvonnan kannalta merkittävää tietoa esimerkiksi kyberturvallisuusvaatimusten laiminlyönnistä ja siinä tehtävästä arviosta, mutta LVV ei saisi kyseisiä tietoja ryhtyäkseen omiin valvontatoimiin.

Mitä tulee ilmoitustoiminnan koordinaatioon ja eri viranomaistehtäviin, Valvira nostaa esille Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen roolin NIS2 -direktiivin 8 artiklan 3 kohdassa tarkoitettuna keskitettynä yhteyspisteenä. Valvira kiinnittää huomiota siihen, että nyt annetussa hallituksen esitys -luonnoksessa ei ole kaikilta osin riittävän painokkaasti huomioitu Kyberturvallisuuskeskuksen keskeistä roolia kyberturvallisuuteen liittyvien poikkeamien käsittelyssä.

Henriksson Markus
Valvira

Lehtonen Niina
Sosiaali- ja terveysalan lupa- ja valvontavirasto Valvira