Directors' Institute Finland - Hallitusammattilaiset ry

Lausunto

28.11.2023

Asia: VN/18157/2023

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

Lausunnonantajan lausunto

Yleiset huomiot NIS2-direktiivin tavoitteista ja tarkoituksesta

Hyvien kyberturvallisuuskäytänteiden kehittäminen EU:n laajuisesti on tärkeää, ja yhtiöiden hallituksilla on merkittävä rooli hyvien kyberturvakäytäntöjen edistämisessä. Samaan aikaan sääntelyn implementaatiossa tulisi huolehtia siitä, ettei hallituksille aseteta direktiivin vähimmäisimplementaatiotasoa korkeampia ja Suomen oikeusjärjestykselle vieraita vaatimuksia. Hallitustyön vaatimuksia ei tulisi lakisääteisesti viedä kohti toimivan johdon velvoitteita, jolloin hallituksen ja johdon välinen työnjako hämärtyy.

Johdon vastuu

Ehdotetun KyberturvallisuusL:n 10§:ssä on käsitelty johdon vastuuta. Ehdotus poikkeaa merkittävästi direktiivistä, jossa säädetään hallintoelinten vastuusta. Suomen osakeyhtiölaissa johto tarkoittaa hallitusta, mahdollista hallinto-neuvostoa ja toimitusjohtajaa. Kun eri direktiiveissä on käytetty termiä hallinto-elin, se on Suomessa säädetty vastaamaan osakeyhtiölain johtoa eli hallitusta, mahdollista hallintoneuvostoa ja toimitusjohtajaa. Osakeyhtiölain mukainen yhtiöoikeudellinen vastuu koskee siis osakeyhtiön johtoa eli osakeyhtiön toimi-elimiä eli hallitusta, mahdollista hallintoneuvostoa ja toimitusjohtajaa. Vastuun ulottaminen toimitusjohtajan välittömässä alaisuudessa kuuluviin tehtäviin (”johtoryhmiin”) on Suomen oikeusjärjestelmälle vieras eikä vastaa direktiivin sanamuotoja. Laajennus olisi merkittävä poikkeus suomalaiseen yhtiöoikeudelliseen sääntelyyn.

Yhtiöoikeudellisen sääntelyn valmistelusta vastaa oikeusministeriö, ja Directors’ Institute Finland – Hallitusammattilaiset ry (DIF) pitää tärkeänä, etteivät muut ministeriöt valmistele omatoimisesti vakiintuneesta yhtiöoikeudellisesta perinteestämme ja osakeyhtiölaista poikkeavia osakeyhtiöissä toimivien henkilöiden vastuu¬säännöksiä. Yhtiöoikeudellisesti hallitus (tai hallintoneuvosto) nimittää

toimitusjohtajan ja valvoo hänen toimintaansa. Toimitusjohtaja taas vastaa yhtiön operatiivisesta johtamisesta ja järjestää sen parhaaksi katsomallaan tavalla. Johtoryhmille ei ole Suomessa asetettu itsenäistä vastuuta ja viittaukset toimitusjohtajan alaisiin (”johtoryhmiin”) tulisi poistaa laki-ehdotuksesta. Toimitusjohtajan suorina alaisina voi työskennellä johtoryhmän jäsenten lisäksi myös muita keskeisessä asemassa olevia johtajia, esimerkiksi sisäisen tarkastuksen tai lakiasiainjohtajia. Yhtiöoikeudellisen vastuun ulottaminen heihin olisi kohtuutonta ja Suomen oikeudelle vierasta.

Kyberturvallisuudesta huolehtiminen on jo nykyisellään osa osakeyhtiölain mukaista hallituksen huolellisuusvelvoitetta, jota tasapainottavat osakeyhtiölain mukaiset vahingonkorvausvelvoitteet. Hallitusten toimintaa ohjaavan liike-toimintapäätösperiaatteen (”business judgement rule”) voidaan katsoa riittävästi turvaavan sitä seikkaa, että hallitus hankkii käyttöönsä asian¬mukaisen osaamisen myös kyberturvallisuusasioista huolellisen päätöksenteon perustaksi. Mikäli näin ei toimittaisi, hallitus olisi vastuussa mahdollisista seuraamuksista osakeyhtiölain vastuurakennelman mukaisesti.

Ehdotuksen 33§:ssä olevien toimintakieltojen soveltamisala on niin ikään hyvin laaja ja aiheuttaa tulkintaepäselvyyttä. Pykälästä tulisi poistaa viittaukset toimitusjohtajan alaisuudessa toimiviin henkilöihin edellä mainituin perustein. Lisäksi edellä mainittu viranomaisvalvonnan jakautuminen useille valvoville viranomaisille voi aiheuttaa epävarmuutta seuraamusjärjestelmän ennakoitavuudesta osakeyhtiön johdossa toimiville. Kuten edellä on todettu, myös ”toimijan” käsite tulisi tältä osin selkeyttää, jotta on selvää, keihin mahdollinen toimintakielto voisi soveltua.

Hallituksen jäsenten rekrytoinnin osalta DIF haluaa nostaa esiin myös sen, että tiettyjen hallituksen osaamisvelvoitteiden nostaminen lakisääteisiksi vaatimuksiksi on omiaan hankaloittamaan pätevien hallitusammattilaisten rekrytointia, nostamaan hallituspalkkioiden tasoa ja kaventamaan käytettävissä olevien hallituskandidaattien piiriä. Hallituksiin kohdistuu jo tällä hetkellä merkittäviä osaamisvaatimuksia erityisesti finanssitoimialalla (ns. fit & proper -vaatimukset). Hallituksen kokoonpanoon vaikuttavat myös muun muassa Hallinnointikoodin riippumattomuusvaatimukset, osakeyhtiölain vaatimus laskentatoimen osaamisesta, sijoittajien over-boarding -vaatimukset (hallitus-paikkojen enimmäislukumääriä koskevat rajoitukset) ja hallituskausien kestoa koskevat vaatimukset sekä jatkossa myös kiintiödirektiiviin perustuvat suku-puolivaatimukset. Mikäli hallituksen jäseniltä edellytetään jatkossa myös operatiivista osaamista kyberturvallisuudesta, tällainen vaatimus kaventaa mahdollisuuksia löytää päteviä hallituskandidaatteja yhtiöihin.

Tulevan sääntelyn myötä kyberturvallisuusasioiden kouluttaminen hallituksille nousee myös yhtiöiden lakisääteiseksi velvoitteeksi. Velvoite on luonteeltaan poikkeuksellinen, eikä vastaavia koulutusvelvoitteita ole asetettu esimerkiksi tietosuojaan, työturvallisuuteen tai muihinkaan hallituksen vastuualueeseen kuuluviin seikkoihin liittyen. Lakisääteisten koulutusvelvollisuuksien laajentaminen jatkossa olisi hallituksen ajankäytön ja toisaalta toimivan johdon sekä hallituksen välisen vastuunjaon kannalta haastavaa, ja tällaisten laki-sääteisten koulutusvaatimusten kansallinen implementointi tulisi rajoittaa direktiivin tarkoittamaan minimiin.

Soveltamisalaa koskevat huomiot

NIS2-direktiivin myötä sääntelyn soveltamisala laajentuu merkittävästi aikaisempaan oikeustilaan nähden.

NIS2-velvoitteiden kohdistumista yritys- ja konsernirakenteessa tulisi selkeyttää. Epäselvää on erityisesti se, tuleeko konsernin emoyhtiön ja/tai kaikkien konsernin tytäryhteisöjen toteuttaa NIS2:n mukaisia velvoitteita, mikäli jokin konserniin kuuluva tytäryhtiö (tai osa siitä) harjoittaa soveltamisalan piiriin kuuluvaa toimintaa. Epäselvää on myös se, lasketaanko ”keskisuuren toimijan” raja-arvot yhteisön itsensä vai koko konsernin tunnusluvuista. Näillä seikoilla ja ”toimijan” käsitteen määrittelyllä on merkittävä vaikutus muun muassa yhtiöiden operatiiviseen varautumiseen ja riskienhallintajärjestelmien luomiseen.

Lisäksi ”toimija”-käsitteen tulkintaepäselvyydet vaikuttavat seuraamus-järjestelmän epävarmuuteen. Ehdotuksessa seuraamusmaksu on sidottu ”toimijan” maailmanlaajuiseen liikevaihtoon, jolloin seuraamusmaksun suuruus voi yhtiörakenteesta riippuen vaihdella merkittävästi, mikäli ”toimijaksi” tulkitaan koko konserni tai yksittäinen tytäryhtiö. Ehdotuksen 33§:n mukaiset liike-toimintakiellot ovat niin ikään sidottu toimimiseen ”toimijan” johtotehtävissä. Tältä osin on epäselvää, voidaanko kyseisiä liiketoimintakieltoja soveltaa esimerkiksi konsernin emoyhtiön hallituksen jäseniin tai toimitusjohtajaan, mikäli NIS2:n mukaista toimintaa harjoitetaan yksittäisessä konsernin tytäryhtiössä.

Riskienhallintavelvoitetta koskevat huomiot

Riskienhallinnalle asetettavien vaatimusten yksi osa-alue on toimitusketjun turvallisuus, mukaan lukien kunkin toimijan ja sen välittömien toimittajien tai palveluntarjoajien välisten suhteiden turvallisuusnäkökohdat (21 artikla: ”-- toimitusketjun turvallisuus, mukaan lukien kunkin toimijan ja sen välittömien toimittajien tai palveluntarjoajien välisten suhteiden turvallisuusnäkökohdat --”). Sana ”välittömien” näyttäisi kuitenkin jääneen pois lakiluonnoksesta. Sanan pois jättäminen johtaisi yhtiöiden kannalta kohtuuttoman laajaan loppu¬tulokseen. Hallituksen esitykseen tulisi näin ollen palauttaa sana ”välittömien”, jolloin lakiluonnos vastaisi direktiivin sanamuotoa ja tarkoitusta.

Raportointivelvoitetta koskevat huomiot

Monikansallisten toimijoiden osalta tulisi selkiyttää sitä, miten toimijoiden ulko-mailla olevat yksiköt huomioidaan NIS2-raportointivelvoitteiden osalta Suomen viranomaisten näkökulmasta. Tähän liittyen on myös huomioitava se, että useilla soveltamisalan piiriin tulevilla yhteisöillä on yksiköitä EU:n alueella sekä kolmansissa maissa.

Valvontaa koskevat huomiot

Ehdotuksessa laiksi kyberturvallisuuden riskienhallinnasta (KyberturvallisuusL) lain velvoitteiden valvonta on jaettu eri viranomaisille sen mukaan, mistä toimi-alasta on kyse. Useat yritykset ja/tai konsernit harjoittavat toimintaa, joka saattaa tulla valvonnan kohteeksi usean viranomaisen toimesta. Tällöin vaarana on valvonnan päällekäisyydestä aiheutuvat tulkintaepäselvyydet. Epäselvyyttä voi aiheuttaa esimerkiksi tilanne, jossa viranomaisten antamat neuvot eroavat saman konsernin/yhteisön/yksikön eri osille.

Myös seuraamusjärjestelmän ennakoitavuus voi kärsiä siitä, että useat eri viranomaiset voivat tehdä seuraamusesityksiä saman konsernin eri yhteisöille. Jos kyse on samasta epäillystä rikkomuksesta ja seuraamusmaksut katsottaisiin laskettavaksi koko konsernin maailmanlaajuisesta liikevaihdosta, tulisi olla selvää, että saman rikkomuksen käsittelyssä ja seuraamusmaksu-arvioinnissa noudatetaan ne bis in idem -sääntöä, eli samasta rikkomuksesta ei langeteta useita päällekäisiä seuraamumaksuja, vieläpä eri maissa.

Seuraamusmaksua koskevat huomiot

Kuten edellä on todettu, ”toimijan” käsitettä tulisi selkeyttää myös seuraamus-maksun määrän ennakoitavuutta silmällä pitäen. Seuraamusmaksun suuruutta määriteltäessä tulisi myös pystyä huomioimaan se, miltä osin toimijan toiminta kuuluu NIS2-direktiivin soveltamisalaan, ja seuraamusmaksua tulisi voida kohtuullistaa NIS2-soveltamisalassa olevan toiminnan laajuus huomioiden.

CSIRT-yksikön tehtäviä koskevat huomiot

Ei ole.

Tiedonhallintalakia ja täytäntöönpanoa julkishallinnossa koskevat huomiot

Ei ole.

Verkkotunnusvälittäjiä koskevat huomiot

Ei ole.

Kumottavaksi ehdotettuja säännöksiä koskevat huomiot

Ei ole.

Vaikutustenarviointia koskevat huomiot

Vaikutusarviointi on puutteellinen. Siinä ei ole lainkaan käsitelty sitä, että ehdotus johdosta poikkeaa merkittävästi direktiivin säännöksistä, jotka käsittelevät hallintoelinten vastuuta, ei toimitusjohtajan alaisuudessa toimiviin henkilöihin. Merkittävä poikkeus yhtiöoikeutemme systematiikasta vaatisi vankat perustelut ja vaikutusarvioinnit, jotka puuttuvat hallituksen esityksestä kokonaan.

Muut huomiot ja avoin palaute esityksestä

Ei ole.

Linnainmaa Leena
Directors' Institute Finland - Hallitusammattilaiset ry