Vauhkonen, Töyrylä-Posio
TIO/TTU

Lausuntoyhteenveto: Luonnos hallituksen esitykseksi kyberturvallisuusdirektiivin (NIS2-direktiivi) täytäntöönpanemiseksi

Liikenne- ja viestintäministeriö pyysi lausuntoja luonnoksesta hallituksen esitykseksi kyberturvallisuusdirektiivin (NIS2-direktiivi) täytäntöönpanemiseksi siten, että suomenkielisen esityksen lausuntoaika oli kahdeksan viikkoa ajalla 3.10.–29.11.2023. Ruotsinkielisen esityksen lausuntoaika oli yhteensä kahdeksan viikkoa siten, että ajalla 6.10.–1.11. ruotsinkielisestä esityksestä oli saatavilla osa esityksestä ja ajalla 1.11.–4.12.2023 koko esitys. Lisäksi esityksestä on pyydetty lausunto Ahvenanmaan maakuntahallitukselta, jolle varattu lausuntoaika on ollut kahdeksan viikkoa ajalla 2.11.–29.12.2023.

Lausuntoja vastaanotettiin määräaikaan mennessä 123 kappaletta. Lisäksi määräajan jälkeen vastaanotettiin 8 kappaletta lausuntoja.

Lausunnonantajista kahdeksalla ei ollut lausuttavaa esityksestä.

Yleiset huomiot NIS2-direktiivin tavoitteista ja tarkoituksesta

Esityksen tarkoitusta ja tavoitteita pidettiin yleisesti kannatettavina. Lausunnoissa todettiin, että yhteiskunnan perustoimintojen kannalta kriittisten toimijoiden viestintäverkkojen ja tietojärjestelmien turvallisuus on muuttunut yhä tärkeämmäksi ja keskeisemmäksi suojelun kohteeksi.

Lausunnoissa pidettiin yleisesti tärkeänä ja ajankohtaisena, että toimenpiteitä kyberturvallisuuden vahvistamiseksi yhteiskunnassa toteutetaan. Ehdotetun sääntelyn uskotaan parantavan tietoturvan tasoa yhteiskunnan toiminnan kannalta kriittisillä toimialoilla. Eri sektoreille asetettavat yhdenmukaiset vaatimukset nähtiin välttämättöminä sekä yhteiskunnan turvallisuuden että yritysten liiketoiminnan näkökulmasta. Yleisesti hyvänä pidettiin myös sitä, että kyberturvallisuustasoa kehitetään tietyillä toimialoilla koko EU:n laajuisesti.

Uutta kyberturvallisuuden riskienhallinnasta annettavaa yleislakia pidettiin yksimielisesti perusteltuna sääntelyratkaisuna sektorikohtaisesti hajautettuun sääntelyyn verrattuna. Lausunnoissa katsottiin yleislain yhteisten riskienhallinta- ja raportointivelvoitteiden yhdenmukaistavan sääntelyn täytäntöönpanoa eri toimialoilla ja kiinnittävän organisaatioiden huomiota kyberturvallisuutta koskevista perusasioista huolehtimiseen nykyistä tehokkaammin. Lisäksi aiempaa verkko- ja tietoturvadirektiiviä merkittävästi laajemman soveltamisalan katsottiin puoltavan keskitettyä yleislakia velvoitteista. Useat lausunnonantajat pitivät perusteltuna, että julkishallinnon osalta täytäntöönpanosta säädettäisiin julkisen hallinnon tiedonhallinnasta annetussa laissa. Muutama lausunnonantaja esitti, että tulisi kuitenkin vielä harkita myös julkishallinnon toimialan säännösten sijoittamista kyberturvallisuuden riskienhallinnasta

annettavaan lakiin tai vaihtoehtoisesti julkishallinnon uuteen erityislakiin. Uuden tiedonhallintalain 4 a luvun ja kyberturvallisuuden riskienhallinnasta annettavan lain keskinäistä suhdetta toivottiin joka tapauksessa kuitenkin vielä selkeytettävän.

Useat lausunnonantajat näkivät vaatimukset tasoltaan kohtuullisena soveltamisalan kohteena oleville toimijoille erityisesti riskienhallinnan osalta. Useammassa lausunnossa kuitenkin todettiin, että yrityksille ja julkishallinnon toimialan toimijoille asetettavat uudet velvoitteet aiheuttaisivat myös hallinnollista taakkaa erityisesti raportointivelvoitteen määräaikojen ja riskienhallinnan dokumentoinnin osalta. Useissa lausunnoissa pidettiinkin hyvänä, että NIS2-direktiivi esitettäisiin täytäntöön pantavaksi vähimmäistasolla eli ilman direktiivin edellyttämiä vaatimuksia korkeampia tai tiukempia velvoitteita. Elinkeinoelämän keskusliitto ja Kyberala ry pitivät tärkeänä, että myöskään viranomaisten tarkentavat määräykset eivät korota vaatimustasoa, vaan olisivat tasapainossa muiden EU-jäsenvaltioiden kanssa.

Maa- ja metsätalousministeriö lausui, että NIS2-direktiivin toimeenpanon yhteydessä on hallitusohjelman mukaisesti varmistettava, että yrityksiin kohdistuva sääntely on selkeää, ennakoitavaa, oikeasuhtaista, kilpailu- ja teknologianeutraalia ja innovaatiomyönteistä. Lisäksi useat lausunnonantajat pitivät tarpeellisena, että direktiivin täytäntöönpanosta ja sen soveltamisalasta laaditaan ohjeistusta niin viranomaisille kuin velvoitteiden piiriin kuuluville toimijoille.

Muun muassa Maanmittauslaitoksen mukaan sääntelyssä on tunnistettu hyvin kyberturvallisuuden hallinnassa välttämätön yhteistyö ja muiden toimijoiden osaamisen hyödyntäminen ja verkostoituminen. Elinkeinoelämän keskusliitto piti tärkeänä, että direktiivin täytäntöönpanossa huomioidaan kansalliset erityispiirteet kuten se, että huoltovarmuusyhteistyö on pitkäaikaisesti perustunut siihen osallistuvien yritysten kannalta ennen kaikkea osapuolten keskinäiseen luottamukseen. Velvoittavan sääntelyn täytäntöönpanossa on syytä huomioida, ettei pitkäaikaisesti ja määrätietoisesti rakennettu luottamus kärsisi.

Ahvenanmaan maakuntahallitus totesi, että NIS2-direktiivin soveltamisalan osalta lainsäädäntövalta jakautuu maakunnan ja valtakunnan kesken. Maakuntahallituksessa on valmisteltu lainsäädäntöä julkishallinnon tiedonhallinnasta, ja alustavasti onkin arvioitu, että tiedonhallintalain 4 a lukuun ehdotettavia säännöksiä vastaavat säännökset voitaisiin sisällyttää myös maakunnassa valmisteltavana olevaan lainsäädäntöön. Maakunnan lainsäädännön jatkovalmistelussa olisi edelleen selvennettävä, miten NIS2-direktiivi täytäntöön pannaan mahdollisimman tarkoituksenmukaisesti ja yksinkertaisesti maakunnan lainsäädäntötoimivaltaan kuuluvalta osin. Koska ehdotettu valtakunnan lainsäädäntö muodostaa integroidun ja monimutkaisen kokonaisuuden, jatkovalmistelussa olisi selvitettävä tarkemmin, onko maakunnan NIS2-direktiivin täytäntöönpanoa ja hallintotehtävien hoitamista tarpeen sovittaa yhteen maakunnan ja valtakunnan välillä.

Soveltamisalaa koskevat huomiot

Lausunnoissa pidettiin yleisesti ottaen tärkeänä, että soveltamisalan määräytyminen olisi mahdollisimman selkeä ja että toimijat pystyisivät itsenäisesti arvioimaan, kohdistuvatko ehdotetut velvoitteet niiden toimintaan ja missä laajuudessa. Useat lausunnonantajat pitivät kuitenkin lain kyberturvallisuuden riskienhallinnasta soveltamisalan määräytymistä vaikeaselkoisena. Soveltamisalaa toivottiin selkeytettäväksi direktiivin mahdollisuuksien sallimissa rajoissa.

Lausunnoissa todettiin, että perustuslain 80 §:n 1 momentin ja 18 §:n sekä yleisemminkin yksilöiden ja yhteisöjen oikeusaseman kannalta olisi suositeltavaa, ettei lain soveltamisala jäisi niin monipolvisen määrittelyn varaan. Lausunnoissa toivottiin selkeytystä muun muassa 4 §:n soveltamisalarajaukseen, kokorajojen määrittelyyn ja velvoitteiden kohdentamiseen konsernien sisällä sekä valtion erityistehtäväyhtiöiden asemaan. Useat lausunnonantajat näkivät tarpeelliseksi, että NIS2-direktiivin artiklassa 2 viitatun suosituksen 2003/361/EY liitteen sekä NIS2-direktiivin johdantolauseen 16 perusteella selvennettäisiin säännösten soveltuvuutta suosituksen mukaisissa omistusyhteys- ja sidosyritystilanteissa tai muutoin konsernirakenteessa.

Myös vaatimusten soveltuminen kansainvälisen monialalayrityksen toiminnassa herätti epäselvyyttä. Lausunnoissa esitettiin, että monet yritykset toimivat kansainvälisesti, mikä voi tehdä paikallisen lainsäädännön yhteensovittamisesta muiden lainkäyttöalueiden lakien ja määräysten kanssa haastavaa etenkin, jos niissä on merkittäviä eroja. Lisäksi epätoivottavana pidettiin tilannetta, jossa yritys joutuisi raportoimaan samasta poikkeamasta useiden jäsenvaltioiden NIS-viranomaisille sekä tilannetta, jossa niiden jäsenvaltioiden, joissa sillä on toimintaa, kansalliset NIS-direktiiviin perustuvat vaatimukset poikkeavat toisistaan.

Yhdessä lausunnossa pyydettiin lisäksi kiinnittämään huomiota erityisesti tiettyihin määritelmiin (keskeinen/keskisuuri/tärkeä toimija) jotta viranomaisen ja toimijoiden välisiltä tulkintaeroilta vältyttäisiin. Joissakin lausunnoissa esimerkiksi katsottiin, että se, ettei esityksessä käytetä NIS2-direktiivissä olevaa ”tärkeän toimijan” määritelmää, voi aiheuttaa epäselvyyttä ohjeistuksen antamisen, noudattamisen tai EU-täytäntöönpanosääntelyn soveltamisen yhteydessä.

Useissa lausunnoissa katsottiin, että esityksestä ei käy riittävän selkeästi ilmi, soveltuisiko sääntely organisaatioon kokonaisuudessaan vai vain siihen osaan organisaatiota, joka harjoittaa soveltamisalaan kuuluvaa toimintoa. Osa lausunnonantajista katsoi, että toimijan kokokriteerin täyttymistä tulisi arvioida vain soveltamisalaan kuuluvan toiminnan osalta. Vastaavasti riskienhallintavaatimusten tulisi kohdistua vain soveltamisalan mukaista toimintaa harjoittavaan organisaation osaan. Kuntaliitto esitti kokokriteerin arviointiin liittyviä huomioita, ja huolen siitä, että soveltamiskriteeristön tulkinta johtaisi epätarkoituksenmukaisen laajaan soveltamiseen vesihuolto- ja jätealalla. Kunnallisissa vesihuoltolaitoksissa kuten kunnan taseyksiköissä ja kunnallisissa liikelaitoksissa soveltamisala voisi olla tarkoituksenmukaisempaa kirjata siten, että toimijana arvioitaisiin vesihuoltolaitosta ja sen kokoa kunnan sijaan. Myös maa- ja metsätalousministeriö kiinnitti huomiota samaan seikkaan ja ehdotti, että lakiin kirjataan poikkeussäännös tai tarkennus niiltä osin, kun toimiala on osa kunnan omaa palveluntuotantoa. Vesihuoltolain mukaan kunnan tulee kirjanpidossaan eriyttää vesihuolto muista toiminnoista, joten on mahdollista tunnistaa keskeiset ja keskeistä pienemmät vesihuoltotoimijat suoraan.

Yhdessä lausunnossa kannatettiin ehdotusta siitä, että valtioneuvoston asetuksella voitaisiin määritellä, että tietyt toimijat kuuluisivat koosta riippumatta lain soveltamisalaan. Oikeusministeriö kuitenkin katsoi, että ehdotettu asetuksenantovaltuus merkitsisi lain soveltamisalan määrittämistä asetuksella, eikä siksi olisi perustuslain näkökulmasta mahdollinen. Säännöstä olisi välttämätöntä tarkentaa siten, että riittävät perussäännökset perustuslain 80 §:n ja 8 §:n edellyttämällä tavalla ovat laissa.

Yhdessä lausunnossa esitettiin, että kansallisen liikkumavaran ulottamista julkishallinnon paikallistason toimijoihin tulisi harkita, sillä tällaiset toimijat voivat käsitellä merkittäviäkin määriä henkilötietoja tai muuta yksityisyyteen liittyvää tietoa, minkä jäämistä velvoitteiden ulkopuolelle ei voida pitää kannatettavana koko yhteiskunnan kyberturvallisuuden kannalta.

Osassa lausuntoja korostettiin, että huoltovarmuuteen tai kyberturvallisuuteen liittyvän sääntelyn ja valvonnan pitäisi kohdistua vain yhteiskunnallisesti merkityksellisiin yrityksiin. Huoltovarmuuskeskus katsoi lausunnossaan, että sääntely ei koskisi rakennetun ympäristön alaa tai yksityistä turva-alaa, mutta että näiden alojen kybervarautuminen olisi hyvä huomioida lainsäädännössä, sillä kyseisten toimialojen häiriöt voisivat vaikuttaa voimakkaasti yhteiskunnan kriittisiin toimintoihin. Ympäristöministeriö puolestaan totesi, että vaikka NIS2-direktiiviä ei sovellettaisi rakennettuun ympäristöön, eli rakentamiseen sekä alueiden käyttöön, rakennettu ympäristö voi kuitenkin tulla direktiivin kansallisen soveltamisalan piiriin osana kriittisen infrastruktuurin tunnistamisen ja kriisinkestävyyden parantamisen lainsäädäntöhanketta, jossa pannaan täytäntöön EU:n CER-direktiivi.

Yhdessä lausunnossa katsottiin, että soveltamisalasta olisi tärkeää tehdä vertailu muihin EU-maihin tai ainakin muihin pohjoismaihin sen arvioimiseksi, että onko soveltamisala määritelty samoin.

Jäljempänä toimialakohtaiset huomiot –osiossa sekä tiedonhallintalakia ja täytäntöönpanoa julkishallinnossa koskevassa jaksossa on esitetty myös soveltamisalaan liittyviä toimialakohtaisia huomioita edellä esitettyä täydentäen.

Riskienhallintavelvoitteita koskevat huomiot

Riskienhallinnan sääntelytapaa, eli toimijoiden velvoitetta itse tunnistaa riskejä ja määritellä sen perusteella tarpeellisia riskienhallintatoimenpiteitä, pidettiin lähtökohtaisesti hyvänä. Täytäntöönpanon aikana toivottiin varmistettavan kuitenkin myös riittävä dialogi toimijoiden ja valvovan viranomaisen välillä. Täytäntöönpanossa toivottiin myös viranomaisen ohjeistusta ja tukea riskienhallintavelvoitteen täyttämiseksi erityisesti sen osalta, millaiset riskinhallintatoimenpiteet arvioidaan oikeasuhtaisiksi ja riittäviksi.

Riskienhallintavelvoite nähtiin lausuntopalautteessa yleisesti määritellyksi sopivalla tarkkuustasolla ja vaatimusten laajuuden todettiin edustavan yleisesti käytössä olevien kyberturvallisuuden viitekehysten näkökulmasta valtavirtaa. Osa lausunnonantajista piti ehdotetun 9 §:n perusteluja liian yksityiskohtaisina, kun taas osa lausunnonantajista piti ehdotettuja velvoitteita liian tulkinnanvaraisina. Yhdessä lausunnossa todettiin, että esitys poikkeaa useista voimassa olevista laeista siinä, että muussa sääntelyssä on tyypillisesti asetettu vain yleinen velvoite huolehtia riittävästä riskienhallinnasta, mutta ei ole yksityiskohtaisesti kerrottu mitä riskienhallinnan tulisi käsittää.

Riskienhallintavelvoitteen osalta nähtiin yleisesti ottaen hyvänä myös, että sääntely on teknologianeutraalia ja että toimijoille jätetään liikkumavaraa toteutustapojen osalta. Osassa lausuntoja kuitenkin toivottiin myös, että laissa nimenomaisesti viitattaisiin kansainvälisesti tunnistettuihin tietoturvastandardeihin tai todettaisiin esimerkiksi ISO 27001-standardin mukaisten toimien kattavan sääntelyn vaatimukset. Lausunnoissa pidettiin tärkeänä lähestymistapaa, jossa toimija voi luoda kyberturvallisuuden riskienhallintamallin itse tai hankkia sen ulkoistetusti ja että malli voi olla osa toimijan laajempaa riskienhallintasuunnitelmaa. Tämä nähtiin tärkeäksi muun muassa toimijoiden hallinnollisen taakan vähentämiseksi sekä valvonnan tehostamiseksi.

Lausunnoissa pidettiin hyvänä, että valvovilla viranomaisilla olisi mahdollisuus tarkentaa lain velvoitteita teknisillä määräyksillä, jotta sektorikohtaisia ominaispiirteitä ja alati muuttuvia teknisiä

yksityiskohtia koskevia asioita voidaan joustavasti huomioida. Oikeusministeriö piti lausunnossaan valvovalle viranomaiselle esitettyjä määräyksenantovaltuuksia liian yksityiskohtaisina ja myös muita kuin teknisiä seikkoja sisältävinä.

Lausunnoissa esitettiin palautetta siitä, että osana kyberturvallisuuden riskienhallintaa tulisi huomioida myös rakennettuun ympäristöön kohdistuvia riskejä. Yksi lausunnonantaja ehdotti, että riskienhallintavelvoitteessa huomioitaisiin myös jäännösriskit ja niiden hyväksyntäprosessit sekä riskin siirtäminen ja pitäminen, jotka ovat osa riskienhallinnan käytänteitä. Lisäksi yksi lausunnonantaja katsoi, että esityksessä tulisi huomioida laitevalmistajaan tai palveluntarjoajaan mahdollisesti liittyvät erityiset haavoittuvuudet laajemmin siten, kuin direktiivi edellyttäisi.

Useissa lausunnoissa tuotiin ilmi, että toimitusketjujen turvallisuutta koskeva 9 §:n 4 kohdan säännösmuotoilua tulisi tarkentaa, jotta se vastaisi sisällöltään 21 artiklan 2 kohdan d alakohtaa ja 3 alakohtaa, jotka sillä olisi tarkoitus panna täytäntöön. Lausunnoissa todettiin, että säännös tulisi täsmentää koskemaan vain välittömiä toimittajia tai palveluntarjoajia direktiivitekstiä vastaavasti. Lisäksi yhdessä lausunnossa todettiin, että kohtaa tulisi täsmentää siten, että toimittajien ja palveluntarjoajien tulisi olla merkityksellisiä kyberturvallisuuden riskienhallinnan kannalta. Yhdessä lausunnossa korostettiin myös, että tarvittaisiin yksittäisiä toimijoita laajempaa näkymää toimitusketjujen turvallisuuteen niihin liittyvien riskien ymmärtämiseksi. Lausunnoissa tuotiinkin laajalti esiin toimitusketjujen turvallisuuden hallinnan haasteellisuutta ja erityisiä osaamistarpeita. Useat lausunnonantajat ilmaisivat huolensa siitä, että esityksessä ei ole huomioitu riittävästi pitkien sopimussuhteiden avaamisen riskejä ja pitkäaikaisten teknologioiden tuomia haasteita. Lisäksi haasteena tunnistettiin se, että toimijalla ei välttämättä ole käytössä tehokkaita keinoja vaikuttaa toimitusketjuun. Taloushallintoliitto lausui, että lainsäädännön tulisi mahdollistaa toimintamalli, jossa arvoketjun yritykset voivat toteuttaa yhdessä 9 §:n toimenpiteet, jolloin myös vastuukysymykset koskisivat vain kustakin toimenpiteestä vastaavaa yritystä. Yksi lausunnonantaja piti tarpeellisena täsmentää, kohdentuuko riskienhallintavelvoite valmistussektorin osalta myös valmistettavien tuotteiden kyberturvallisuusominaisuuksiin.

Oikeusministeriö huomautti, että kyberturvallisuuden riskienhallinnasta annetun lain 14 §:n 3 momentin osalta olisi huomioitava, että hallintolain 34 §:ssä säädetään jo viranomaisen velvollisuudesta kuulla asianosaista.

Erityisesti muutaman hyvinvointialueen lausunnossa kiinnitettiin huomiota kyberturvallisuuden riskienhallinnasta ehdotetun lain ja tiedonhallintalain riskienhallintavelvoitteiden muotoilujen eroihin ja toivottiin että lait olisivat mahdollisimman pitkälti samansisältöisiä, jotta vältyttäisiin tulkintaongelmilta tilanteissa, joissa sama toimija kuuluisi sekä kyberturvallisuuden riskienhallinnasta ehdotetun lain että tiedonhallintalain uuden luvun soveltamisalaan.

Lausunnoissa myös esitettiin zero trust-teknologian soveltamiseen ja lainsäädännön johdonmukaisuuteen liittyviä huomioita.

Lausunnoissa toivottiin varmistettavan, että ehdotetun lain velvoitteiden piiriin kuuluvat toimijat, voivat kohtuudella suorittaa henkilöstöä koskevia turvallisuusselvityksiä.

Useissa lausunnoissa tuotiin esiin, että osakeyhtiön hallintoelimille asetettavat pakolliset koulutusvelvoitteet ovat kansallisesti vieraita, ja että sääntelyssä tulisi pitää selkeästi erillään hallituksen valvontarooli ja toimivan johdon rooli. Yhtenä vaihtoehtona esitettiin, että säännöksen yksityiskohtaisiin perusteluihin lisättäisiin velvoitetta selkeyttävä kuvaus toimijan harkintavallasta

todentaa riittävä perehtyneisyys luotettavalla tavalla. Johdon vastuuta koskevaan 10 §:än liittyen useissa lausunnoissa todettiin lisäksi, että vastuun ulottaminen toimitusjohtajan välittömässä alaisuudessa kuuluviin tehtäviin tulisi poistaa, sillä se ei vastaa direktiivin sanamuotoja ja olisi poikkeus suomalaiseen yhtiöoikeudelliseen sääntelyyn. Pykälää pidettiin muuten selkeänä ja hyvin kirjoitettuna sen osalta, mistä johto vastaa.

Useat lausunnonantajat totesivat, että useita ehdotettuja riskienhallintatoimenpiteitä tehdään jo nykyään, mutta sääntelyn myötä niitä tehtäisiin jatkossa perusteellisemmin ja dokumentoitaisiin paremmin. Lausuntopalautteessa nähtiin myös tärkeänä tunnistaa se, että riskienhallinta on jatkuva ja kehittyvä prosessi, joka ei tule koskaan valmiiksi ja että teknologisen ympäristön riskienhallintakin elää ja kehittyy ajan myötä.

Raportointivelvoitteita koskevat huomiot

Ehdotettua kolmiportaista ilmoitusmallia pidettiin selkeänä ja perusteltuna. Lausunnoissa esitettiin huomioita ensi- ja jatkoilmoituksen aikarajoista, joita pidettiin hyvin tiukkoina organisaatioille.

Useat lausunnonantajat pitivät merkittävän poikkeaman määritelmää alttiina tulkintaeroille erityisesti edellytettävän taloudellisen tappion laajuuden osalta. Lausunnoissa nähtiinkin tarpeelliseksi ja osin myös välttämättömäksi merkittävän poikkeaman määritelmää tarkentava valvovan viranomaisen määräys, ohje tai suositus. Oikeusministeriö piti merkittävän poikkeaman määritelmää koskevaa määräyksenantovaltuutta muuna kuin teknisenä määräyksenantovaltuutena, jota viranomaiselle ei tulisi voida osoittaa. Useissa lausunnoissa todettiin, että mikäli raportointivelvoite syntyisi tulkinnallisista syistä jo vähäisten taloudellisten tappioiden vuoksi, johtaisi se epätarkoituksenmukaisen alhaiseen raportointikynnykseen ja pääosin tarpeettomiin ilmoituksiin. Muun muassa oikeusministeriö ehdotti, että merkittävän poikkeaman määritelmää tarkennettaisiin siten, että sillä tarkoitetaan poikkeamaa, joka on aiheuttanut tai voi aiheuttaa merkittäviä taloudellisia tappioita. CSC - Tieteen tietotekniikan keskus Oy puolestaan ehdotti, että merkittävä poikkeama rajattaisiin tilanteisiin, joissa on suuri todennäköisyys sille, että palveluille aiheutuu vakava toimintahäiriö tai asianomaiselle toimijalle taloudellisia tappioita.

Myös kyberuhkien ja läheltä piti –tilanteiden määritelmiä pidettiin haastavina ja alttiina tulkinnoille. Kyberuhka on laaja käsite, joten pykälän perusteella ei ole selvää, mistä pitäisi ilmoittaa ja mistä ei. Kyberuhkien sijaan ehdotettiin puhuttavan esimerkiksi haavoittuvuudesta. Läheltä piti-tilanteiden osalta koettiin puolestaan vaikeaksi tulkita, mikä on jotain, mikä olisi voinut olla riski, jos mitään ei ole vielä tapahtunut.

Yksi lausunnonantaja huomautti, että kun IT-ympäristöt toteutetaan tyypillisesti alihankintaketjujen avulla, on odotettavissa ilmoituksia sekä toimittajalta että sen asiakkaalta silloin, kun tietoturvapoikkeama kohdistuu tietoteknisen palvelun toimittajaan.

Lausunnoissa pidettiin tärkeänä, että ilmoitusten tekemiseen on olemassa sähköinen ja helppo kanava. Yhdessä lausunnossa toivottiin, että raportointityökalu ohjaisi yhteismitallisuuteen ja raportoinnin seurattavuuteen. Käytännön syistä toivottiin, että raportti voitaisiin tehdä myös englanniksi. Lausunnoissa pidettiin lisäksi tärkeänä, että ilmoittaja saisi itse tallennettua lähetetyn ilmoituksen aikaleimoineen ja ilman erillistä pyyntöä. Lausunnoissa pidettiin hyvänä, että ilmoitusten tekemiseen tarkoitettu palvelu välittäisi ilmoituksen tiedot suoraan CSIRT-yksikölle

ilman, että valvovan viranomaisen tarvitsisi erikseen välittää ilmoitusta. Ilmoitusten automaattinen siirtyminen CSIRT-yksikölle tulisi varmistaa erityisesti virka-aikojen ulkopuolella ja ilmoituskanavan toivottiin muutenkin mahdollistavan automaation hyödyntämisen raportointimenettelyn keventämiseksi. Verohallinto pitää tärkeänä, että ennen ilmoittamismenettelyn aloittamista ilmoittamisesta vastuussa oleville tahoille annetaan menettelyohjeet siitä, miten ilmoitukset annetaan teknisesti oikein. Menettelyn suunnittelussa tulisi hyödyntää Tietosuojavaltuutetun kokemuksia tietoturvaloukkaus ilmoitusten vastaanottamisessa.

Sisäministeriö korosti lausunnossaan, että poikkeamissa voi olla kyse rikoksista, joissa on korkea selvittämisintressi sekä yksilön että yhteiskunnan kannalta. Sisäministeriö ehdotti, että samalla ilmoituksella tulisi voida tehdä NIS2-ilmoitus, CER-direktiivin mukaiset ilmoitukset sekä rikosilmoitus. Poliisihallitus esitti niin ikään lausunnossaan, että poikkeamailmoitusten myötä valvovalle viranomaiselle voisi kertyä tietoja vakavistakin teoista, joiden epäillään aiheutuvan rikoksesta, mutta valvovalla viranomaisella ei olisi velvoitetta ilmoittaa niistä poliisille, mitä ei voida pitää tarkoituksenmukaisena. Poliisihallitus katsoo, että CSIRT-yksiköllä tulisi olla velvollisuus ilmoittaa tieto poliisille merkittävistä kyberpoikkeamista.

Useat lausunnonantajat toivoivat, että useampia erilaisia raportointeja voitaisiin tehdä keskitetyn kanavan kautta (tietosuoja-asetus, NIS2-direktiivi, E-Privacy -direktiivi ja CER-direktiivi). Elinkeinoelämän keskusliitto korosti lausunnossaan, että raportoinnissa tulisi ehdottomasti pyrkiä ”yhden luukun periaatteeseen” ensin kansallisesti ja pidemmällä aikavälillä koko EU:ssa. Lisäksi Tuomioistuinviraston lausunnossa todettiin, että ilmoitustoiminnallisuuden lisäksi kanavaan voisi keskittää organisaatiolle osoitetut toimintaohjeet poikkeamatilanteen hallinnan ja hoitamisen osalta huomioiden tietosuojan, tiedonhallinnan, tietoturvan ja riskienhallinnan näkökulman. Tuomioistuinvirasto toteaa lisäksi, että myös viranomaisten välisiä toimintaprosesseja olisi syytä kehittää siten, että asiakasrajapinta ilmoittajille olisi mahdollisimman yksinkertainen, mutta samalla tehokkaat viranomaisprosessit käynnistävä.

Yksi lausunnonantaja katsoi, että kolmiportaisen raportoinnin toteuttaminen voi osoittautua haastavaksi organisaatiolle, jos se ei ole aiemmin soveltanut toiminnassaan tietoturvan tai kyberturvallisuuden hallintamallia. Erityisesti velvoite raportoida merkittävästä poikkeamasta 24 tunnin kuluessa arvioitiin haastavaksi toteuttaa, jos toimijalla ei ole ympärivuorokautista toimintaa tai valvontaa. Raportointivelvoitteen määräajan kuluminen käynnistyisi ehdotuksen mukaan merkittävän poikkeaman havaitsemisesta. Lausunnoissa toivottiin lisäksi esityksen täsmentämistä siltä osin, milloin toimijan katsotaan havainneen poikkeaman.

Useat lausunnonantajat erityisesti julkisen sektorin organisaatioissa pitivät esitettyä 24 tunnin aikarajaa ensi-ilmoituksen tekemiselle haastavana. Myös jatkoilmoituksen tekemiselle asetettu aikaraja koettiin tiukaksi. Yksi lausunnonantaja pitää myös loppuraportoinnille asetettua kuukauden määräaikaa liian lyhyenä ainakin silloin, jos hyökkäys kestää pitkään tai tilannekuva täydentyy vielä merkittävänkin ajan kuluttua. Yksi lausunnonantaja totesi, että erityisesti tilanteissa joissa samaa organisaatiota valvoisi useampi viranomainen, raportointivelvoitteen toteuttaminen vaatii suunnittelua ja velvoitteiden selventämistä.

Monikansallisten toimijoiden osalta toivottiin selkiytystä siitä, miten muualla EU:ssa tai kolmansissa maissa sijaitsevat yksiköt tulisi huomioida NIS2-direktiivin mukaisten raportointivelvoitteiden osalta Suomen lainsäädännön näkökulmasta. Yhdessä lausunnossa todettiin, että yrityksen kannalta on kohtuutonta, että samasta tietoturvaloukkauksesta tulee raportointivelvoitteita tietosuoja- ja tietoturvaviranomaisille useissa EU-jäsenvaltioissa.

Energiavirasto pitää tärkeänä, että valvovalle viranomaiselle on annettu ehdotetun 12 §:n nojalla oikeus pyynnöstä saada lisätietoja tai väliraportti poikkeaman tilannepäivityksistä ja käsittelyn edistymisestä. Energiavirasto katsoo kuitenkin, että poikkeamahallintaan liittyviä tiedonsaantioikeuksia tulisi uudelleen tarkastella, erityisesti CSIRT-yksikön ja valvovan viranomaisen välisen tiedonvaihdon sekä valvovan viranomaisen ja tietosuojavaltuutetun välisen tiedonvaihdon osalta.

Yksi lausunnonantaja esitti, että erityisesti laajoihin vahinkoihin johtaneet tilanteet edellyttävät pelkkää tietoturvaloukkausta laajempaa tutkintaa, jollaiseen on onnettomuuksien ja poikkeuksellisten tapahtumien tutkinnassa totuttu.

Yksi lausunnonantaja lausui 14 §:n 2 momentin velvoitteen liittyen kyberuhkasta tiedottamiseen palvelujen vastaanottajille olevan tulkittavissa tarpeettoman laajasti esimerkiksi vesihuollon osalta, jossa palvelun vastaanottajia ovat käytännössä kaikki asukkaat.

Osalle lausunnonantajista oli jäänyt epäselväksi, tulisiko valvovien viranomaisten järjestää ympärivuorokautinen päivystys poikkeamailmoitusten vastaanottoa ja käsittelyä varten, vai kuuluisiko tällainen päivystysvelvoite keskitetysti Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen vastuulle. Lausunnoissa todettiin, että Liikenne- ja viestintäviraston nykyinen valtionhallinnolle ja huoltovarmuuskriittisille toimijoille tarkoitettu 24/7- päivystys tulee ehdottomasti säilyttää ja myös toimialakohtaisilla valvovilla viranomaisilla voisi olla velvollisuus 24/7-päivystyksen järjestämiseen. Osa lausunnonantajista toivoi raportoinnilta kaksisuuntaisuutta, eli että myös viranomaiset olisivat velvollisia raportoimaan toimijalle tai jakamaan anonymisoituja tietoja merkittävistä poikkeamista muille soveltamisalaan kuuluville toimijoille. Yhdessä lausunnossa toivottiin, että luovutettaessa tietoja viranomaisten kesken, tulisi asiasta ilmoittaa aina sille yritykselle, jonka tietoja on luovutettu.

Lausunnoissa pidettiin tärkeänä huolehtia siitä, että Liikenne- ja viestintävirastolla on riittävät resurssit myös vapaaehtoisten ilmoitusten käsittelemiseksi, jotta toimijoilla olisi riittävät kannustimet tehdä vapaaehtoisia ilmoituksia.

Maa- ja metsätalousministeriö katsoi, että esityksessä poikkeaman käsittelyn ja poikkeamailmoitusten käsittelyn määrittely ja keskinäinen suhde vaatisi määritelmien selkeyttämistä tai täsmentämistä.

Valvontaa koskevat huomiot

Useat lausunnonantajat, sekä viranomaiset että velvoitteiden soveltamisalaan kuuluvien organisaatioiden edustajat, kannattavat hajautettua valvontamallia etenkin huomioiden soveltamisalan laajuus ja monimuotoisuus. Toiminnan turvallisuuden arviointia kokonaisuutena pidettiin laajalti tarkoituksenmukaisena ja valvovalta viranomaiselta toivottiin ymmärrystä sekä valvottavasta toimialasta että kyberturvallisuudesta. Hajautetun valvonnan todettiin myös tukevan kyberturvallisuuden vastuunjakoa Suomessa, jossa kyberturvallisuuteen liittyviä viranomaisvastuita ei ole keskitetty yhdelle toimijalle vaan kyberturvallisuus on osa kaikkien toimialojen tekemistä. Oikeusministeriö kuitenkin pitää hajautettua valvontamallia ongelmallisena arvioitaessa esimerkiksi kyberturvallisuuden valvontatehtävän horisontaalista merkitystä (vrt. tietosuojalainsäädännön noudattamisen valvonta), oikeusturvan toteutumista ja esitysluonnoksessa kaavailtua

viranomaisen norminantovaltaa. Oikeusministeriö pitäisi perusteltuna arvioida vaihtoehtoisena toteutustapana valvontatehtävän keskittämistä Liikenne- ja viestintävirastolle.

Työ- ja elinkeinoministeriö lausuu, että valvontatehtävien jakoa eri viranomaisille olisi hyvä tarkastella uudelleen myöhemmin, jos havaitaan esimerkiksi päällekkäisyyksiä yrityskohtaisesti viranomaisten toimivaltuuksissa. Lausuntokierroksen aikana ei ole ollut käytettävissä tietoa siitä, mitä CER-kriittiset toimijat tai niitä valvovat viranomaiset tulisivat olemaan, minkä vuoksi esitykseen olisi vaikea lausua tältä osin liittyen valvontatehtäviin. Eduskunnan oikeusasiamies piti sektorikohtaisesti hajautettua valvontamallia koskevaa arviota monipuolisena, eikä näe siinä huomauttamista. Esityksessä tulisi kuitenkin kiinnittää huomiota myös valvonnan riippumattomuuteen arvioitaessa viranomaisen ja yksityisen sektorin välistä yhteistyötä. Eduskunnan oikeusasiamiehen mukaan voi olla lisäksi tarvetta selkiyttää 1. lakiehdotusten valvontasäännösten suhdetta oikeusasiamiehen kanslian toimintaan ylimpänä laillisuusvalvojana. Esimerkiksi tiedonhallintalain 3 §:ssä on otettu huomioon valtioneuvoston oikeuskanslerin asema ylimpänä laillisuusvalvojana asianmukaisella tavalla ja jätetty oikeuskansleri Liikenne- ja viestintäviraston valvonnan ja seuraamusten ulkopuolelle.

Sosiaali- ja terveysalan lupa- ja valvontavirasto Valvira sekä Lääkealan turvallisuus- ja kehittämiskeskus Fimea katsovat, että sektorikohtainen valvonta ei Valviran ja Fimean osalta jakaudu esityksessä selkeästi määritellyllä tavalla, eikä vastaa nykyistä sääntelyä. Lausunnoissa todetaan, että soveltamisalaa sekä valvontavastuun jakautumista terveyssektorilla olisi syytä tarkentaa siten, että terveysalan toimijoiden valvonta keskitettäisiin Valviralle ja lääke- ja apteekkialan toimijoiden valvonta Fimealle. Vastaavia huomioita esittivät Suomen Apteekkariliitto ja eräät muut terveyssektorin lausunnonantajat. Terveyssektorin valvontavastuun tarkentamistarve tuotiin esiin myös hyvinvointialueiden lausunnoissa.

Työ- ja elinkeinoministeriö sekä Energiavirasto lausuivat pitävänsä tarkoituksenmukaisempana, että vedyn siirtoa harjoittavia toimijoita valvoisi Turvallisuus- ja kemikaaliviraston sijasta Energiavirasto. Lisäksi Säteilyturvakeskus ehdottaa harkittavaksi jatkovalmistelussa, että Säteilyturvakeskus olisi valvontaviranomainen ydinvoimalaitosten osalta, sillä se valvoo jo nykyisin ydinvoimalaitosten tietoturvallisuutta ydinenergialainsäädännön mukaisesti.

Valvonnan tehokkuuden ja vaikuttavuuden kannalta pidettiin tarkoituksenmukaisena, että valvonnasta säädetään riskiperusteisuutta painottaen. Myös valvonnan jakaminen keskeisten toimijoiden etukäteisvalvontaan ja tärkeiden toimijoiden jälkikäteisvalvontaan nähtiin hyvänä ja hallinnollista taakkaa keventävänä ratkaisuna. Yhdessä lausunnossa arvioitiin, että kynnys valvoa muita kuin keskeisiä toimijoita on asetettu varsin korkeaksi. Lisäksi yhdessä lausunnossa todettiin, että tärkeiden toimijoiden jälkikäteisvalvontaa koskeva kohta on muotoiltu epäselvästi. Yhdessä lausunnossa todettiin myös, että esityksestä ei saa selkeää kuvaa siitä, kuinka valvonta toteutettaisiin käytännössä ja mitä se pitäisi sisällään.

Yhdessä lausunnossa ehdotettiin, että valvova viranomainen voisi antaa määräyksiä ehdotetun 27 §:n tiedonsaantioikeuksien osalta. Myös oikeusministeriö katsoi, että sekä valvovan viranomaisen, että seuraamusmaksulautakunnan tiedonsaantioikeuksia tulisi vielä tarkentaa. Poliisihallitus arvioi, että valvovan viranomaisen tiedonsaantioikeuden toteuttaminen siten, että valvova viranomainen vaatisi tiedot tietyssä muodossa voi olla käytännössä vaikea toteuttaa, jos vaadittu muoto on esimerkiksi jonkin ohjelmiston edellyttämä tietomuoto. Elinkeinoelämän keskusliitto ehdotti lausunnossaan, että tietojen luovuttamisen kustannukset olisi korvattava toimijoille ja että toimijalla tulisi olla oikeus kieltäytyä tietojen luovuttamisesta, jos taakka olisi kohtuuton. Lisäksi

oikeusministeriö kommentoi 28 §:n mukaista tiedonsaantioikeutta ja sitä koskevia säätämisjärjestysperusteluja. Oikeusministeriön näkemyksen mukaan säännös vaikuttaisi sen sisältöiseltä, että luottamuksellisen viestin salaisuuden suojaa nauttivaa viestintää saatettaisiin myös valvonnallisista syistä rajoittaa. Tältä osin oikeusministeriö katsoi, että esitystä tulisi tarkentaa ja täsmentää perustuslain 10 §:n 4 momentin erityisten rajoitusedellytysten täyttymisen osalta, perustuslakivaliokunnan kannanottojen osalta sekä kansallisen liikkumavaran osalta.

Oikeusministeriö piti tarpeellisena tehdä tarkastusoikeutta koskevaan säännökseen tarkennuksia, muun ohella sitä, että turvallisuusjärjestelyjen tarkastusoikeus tulisi tehtävän luonteen ja merkityksen vuoksi säilyttää viranomaisella, eli sitä ei tulisi voida siirtää ulkopuoliselle asiantuntijalle. Lisäksi muissa lausunnoissa esitettiin ulkopuolisen tarkastajan turvallisuusselvityksiin liittyviä huomioita. Kyberala ry esitti, että tarkastuksia koskevaa säännöstä tulee tarkentaa niin, että dataan, tietoon ja tietojärjestelmiin oikeuttavan pääsyn ja muiden käytänteiden, mukaan lukien viranomaisen lukuun toimivan tahon roolin on perustuttava myös toimijan suostumukseen. Perusteluna on todettu, että direktiivin mukaan viranomaisella on oikeus ainoastaan esittää pyyntö pääsystä dataan ja tietoihin. Kyberala ry:n mukaan olisi lain tarkoitusperien vastaista velvoittaa toimijaa luovuttamaan kolmannelle osapuolelle oikeudet tietojärjestelmiin ja tietoihin.

Oikeusministeriö esitti lisäksi useita muutos- ja täydennystarpeita luvanvaraisen tai sertifioidun toiminnan rajoittamista sekä luvan tai sertifioinnin peruuttamista koskevaan säännökseen. Samaan säännökseen liittyen myös työ- ja elinkeinoministeriö sekä Energiavirasto esittivät erityisesti sähkö- ja maakaasuverkkotoiminnan jatkuvuuden turvaamiseen liittyviä huomioita.

Useat lausunnonantajat katsoivat, että ehdotettu muotoilu johdon toiminnan rajoittamisesta menisi direktiivin vähimmäisedellytyksiä pidemmälle, ja että toimivaltuuden ei tulisi koskea toimitusjohtajan välittömässä alaisuudessa toimivia henkilöitä. Elinkeinoelämän keskusliitto piti lisäksi viiden vuoden määräaikaa johdon toiminnan rajoittamiselle poikkeuksellisen ankarana ja edellytti, että kiellon tulisi kestää vain puutteellisen toiminnan ajan siten, että kiellon piiristä vapauduttaisiin, kun puutteet direktiivin noudattamisessa on korjattu.

Oikeusministeriö piti välttämättömänä, että ehdotettua 31 §:ä täsmennettäisiin sekä sääntelyn rikkomisesta tiedottamisen, että huomautuksen ja varoituksen antamisen osalta.

Oikaisuvaatimusmenettelyn todettiin soveltuvan huonosti valvontamenettelyssä annettaviin 31-33 §:n mukaisiin päätöksiin. Nähtiin, että valvontamenettelyssä tehtävät päätökset tulisivat perustumaan perusteelliseen selvitykseen ja menettelyyn, johon kuuluu myös asianosaisten kuuleminen. Kun valvontapäätös annetaan tällaisen perusteellisen selvittämisen ja kuulemisen jälkeen, ei ole oletettavaa, että päätöstä enää muutettaisiin oikaisuvaatimuksen perusteella, minkä johdosta oikaisuvaatimus muodostuisi muutoksenhakuprosessin osalta turhaksi välivaiheeksi ennen hallinto-oikeuden käsittelyä.

Kuntaliitto pitää lausunnossaan tärkeänä, että kyberturvallisuuden yleisvalvonnassa ja mahdollisessa toimijakohtaisessa sanktioinnissa noudatetaan tarkoituksenmukaisia valvonta- ja sanktiointiperiaatteita valvojatahosta riippumatta, jotta varmistetaan eri toimialojen toimijoiden yhdenmukainen kohtelu. Lausuntopalautteessa on myös arvioitu, että eri sektoreiden valvonnan yhteismitallisuus voidaan varmistaa koordinaatiotoimin. Useampi lausunnonantaja esitti huomion, että sen toimintaa tulisi valvomaan useampi kuin yksi valvova viranomainen, koska se harjoittaa toimintaa usealla eri toimialalla. Lausunnoissa toivottiinkin, että valvonnan osalta täsmennettäisiin,

miten monialayhtiöitä valvotaan ja että valvovien viranomaisten yhteistyön tulisi olla siten koordinoitua ja saumatonta, että valvontatoimet ja viranomaisten ohjeet ovat toisiaan täydentäviä eivätkä päällekkäisiä tai ristiriitaisia. Lausuntopalautteessa esitettiin myös huoli siitä, että seuraamusjärjestelmän ennakoitavuus voi kärsiä, jos useat eri viranomaiset voivat tehdä seuraamusesityksiä esimerkiksi saman konsernin eri yhteisöille. Helsingin seudun ympäristöpalvelut kiinnitti valvonnan päällekkäisyyteen liittyen huomiota siihen, että vaikka vesi- ja jätehuollossa olisi esityksessä sama viranomainen, aluehallintoon liittyvän uudistuksen johdosta muutoksia voi tapahtua.

Yksi lausunnonantaja arvioi, että valvonta tulee olemaan haasteellista suuren organisaatiomäärän vuoksi, sillä soveltamisalaan kuuluvien toimijoiden määrä kasvaa moninkertaiseksi NIS1-direktiivistä. Valvovien viranomaisten lisäresursointi nähtiinkin erittäin tärkeänä ja kannatettavana. Lisäresurssitarpeiden lisäksi muun muassa oikeuskanslerin virasto korosti tarvetta huomioida viranomaisten osaamisen syventäminen kyberturvallisuusasioissa, jotta valvontatehtäviä voidaan asianmukaisesti hoitaa. Etenkin valvovien viranomaisten lausunnoissa toivottiin myös viranomaisille riittävää ohjausta ja neuvontaa uusien tehtävien toteuttamiseen. Lisäksi viranomaisten välinen joustava yhteistyö ja tiedonvaihto koettiin tärkeäksi paitsi nyt ehdotetun valvonnan järjestämiseksi, myös huomioiden esimerkiksi tietosuojavaltuutetun toimiston rooli kokonaisuudessa.

Lausuntopalautteessa pidettiin välttämättömänä, että valvontaviranomaiset huolehtivat toimijoiden riittävästä neuvonnasta ja ohjauksesta erityisesti, koska lain 43 §:ssä asetetaan toimijoille velvoite tunnistaa itse asemansa soveltamisalaan kuuluvana ja tehdä ilmoitus, jonka laiminlyönnistä voisi seurata lain 37 §:n nojalla hallinnollinen seuraamusmaksu.

Turvallisuus- ja kemikaalivirasto esittää, että valmistelussa selvitettäisiin mahdollisuuksia laajentaa olemassa olevia järjestelmiä valvovien viranomaisten yhteiseen käyttöön tai perustaa uusi yhteinen ratkaisu toimijaluetteloiden ylläpitoon ja poikkeamailmoitusten vastaanottamiseen ja käsittelyyn. Vastaavasti Turvallisuus- ja kemikaalivirasto katsoo, että kyberturvallisuuden riskienhallinnasta annettavaan lakiin olisi tarpeen lisätä säännökset viranomaisten tietojärjestelmäyhteistyön mahdollistamiseksi. Keskeisenä perusteluna on todettu, että esitettyjen arvioiden mukaan uusien valvontatehtävien hoitamisesta aiheutuu tietojärjestelmäkehityskustannuksia lähes kaikille valvoville viranomaisille. Työ- ja elinkeinoministeriö pitää tärkeänä, että lain toimivuutta ja Turvallisuus- ja kemikaaliviraston resurssien riittävyyttä seurataan.

Seuraamusmaksua koskevat huomiot

Useat lausunnonantajat kannattivat ehdotettua mallia seuraamusmaksulautakunnasta. Oikeusministeriö katsoi yhtyvänsä hallituksen esityksen perusteluihin siitä, että seuraamusmaksujen suuruuden vuoksi monijäseninen päätöksentekoelin on tarpeen.

Seuraamusmaksulautakunnan suhteen lausuntopalautteessa pidettiin tarpeellisena selkeyttää, minkä viranomaisen yhteyteen se perustettaisiin, mikä taho seuraamuslautakuntaa valvoisi, olisivatko lautakunnan jäsenet virkasuhteessa vain nimeävään valvovaan viranomaiseen ja olisiko seuraamusmaksun määräämistä koskevassa esityksessä kyse valvontaviranomaisen vai virkamiehen esityksestä. Yhdessä lausunnossa pyydettiin lisäksi kiinnittämään huomiota jäsenten jääviyttä koskeviin kysymyksiin.

Lausuntopalautteessa kannatettiin laajalti sitä, että julkishallinnon toimijoille ei voitaisi määrätä hallinnollista seuraamusmaksua. Ratkaisu nähtiin perusteltuna ottaen huomioon kansallisessa lainsäädännössä jo noudatettu käytäntö (mm. TietosuojaL 24 §) ja se, että viranomaistoimintaan kohdistuu jo muutoinkin vahvemmat lain noudattamisen velvoitteet ja virkavastuu verrattuna yksityisen sektorin toimijoihin. Kuntaliitto huomautti lausunnossaan, että myös kunnat (ollessaan lain soveltamisalassa), yhtä lailla kuin valtion virastot ja hyvinvointialueet tulee jättää seuraamusmaksujen ulkopuolelle. Lisäksi lausunnoissa pyydettiin tarkentamaan, sovelletaanko seuraamusmaksua kuntien taseyksikköinä, liikelaitoksina, osakeyhtiöinä tai kuntayhtyminä toimiviin vesi- ja jätehuollon toimijoihin. Yksi lausunnonantaja katsoi, että mikäli organisaation tulot ovat pääosin veroista lähtöisin, niin seuraamusmaksua tehokkaampi pelotevaikutus muodostuisi vastuun kohdentamisella siihen, jolla on tosiasiallinen päätäntävalta tietoturvan toteutumisesta julkisessa organisaatiossa.

Kaksi lausunnonantajaa ei pitänyt julkishallinnon rajaamista seuraamusmaksujen ulkopuolelle kannatettavana, vaan näki ratkaisun epäoikeudenmukaiseksi ja johtavan entistä vaikeampiin vastuullisuuskysymyksiin.

Lausunnoissa pidettiin seuraamusmaksujen määrää sekä oikein mitoitettuina ja tarkoituksenmukaisina että liian suurina. Lausunnoissa todettiin, että seuraamusmaksun suuruutta määriteltäessä tulisi huomioida se, miltä osin toimijan toiminta kuuluu NIS2-direktiivin soveltamisalaan, kuinka laajaa toiminta on, kuinka kriittistä toiminta on yhteiskunnan kannalta, tapahtuneen laiminlyönnin vakavuus ja seuraukset sekä toiminnan jatkamisen edellytykset. Lisäksi lausunnoissa toivottiin selvennystä siihen, miten seuraamusmaksun määräämisen osalta menetellään monella toimialalla toimivien yritysten, konserniyritysten tai globaalien yritysten osalta.

Oikeusrekisterikeskuksen näkemyksen mukaan rangaistusluonteisille hallinnollisille seuraamusmaksuille ei tulisi periä viivästyskorkoa, mikä tulisi tarkentaa esitykseen. Oikeusrekisterikeskus pitää yhtä lailla tärkeänä, että sakon täytäntöönpanosta annettua lakia esitettäisiin samalla muutettavaksi siten, että sen soveltamisalaa koskevaan 1 §:n 2 momentin listaan sisällytettäisiin ehdotettu uusi hallinnollinen seuraamusmaksu. Lausunnossa todetaan, että sakon täytäntöönpanosta annetun lain nojalla täytäntöönpantavat uudet rangaistusluonteiset hallinnolliset seuraamukset on viime vuosina säännönmukaisesti lisätty sakon täytäntöönpanosta annetun lain 1 §:n 2 momentin listaan. Oikeusrekisterikeskus piti seuraamusmaksun täytäntöönpanoa koskevaa ehdotusta asianmukaisena.

Tietosuojavaltuutetun toimiston lausunnossa pidettiin tarpeellisena, että esityksessä otettaisiin selkeästi kantaa siihen, onko NIS2-direktiiviä tulkittava siten, että henkilötietojen käsittelyn turvallisuuteen liittyvistä puutteista määrättävät seuraamukset olisivat vain tietosuojavaltuutetun kollegion toimivallassa. Lausunnoissa pidettiin muutoinkin tarpeellisena selkiyttää suhdetta tilanteisiin, joissa tapahtuu myös tietosuojaloukkaus, mikä voisi olla tyypillistä tietoturvaloukkauksen yhteydessä. Oikeuskanslerinviraston lausunnossa katsottiin, että mahdollinen päällekkäisyys tietosuoja-asetuksen 83 artiklassa säädetyn seuraamusmaksun kanssa on otettu asianmukaisesti huomioon säännöstekstissä.

CSIRT-yksikön tehtäviä koskevat huomiot

CSIRT-yksikön sijoittamista Liikenne- ja viestintäviraston Kyberturvallisuuskeskukseen pidettiin lausunnoissa yleisesti perusteltuna. CSIRT-yksikön tehtävät katsottiin laissa riittävästi

määritellyiksi. Oikeusministeriö piti tarpeellisena, että laissa säädettäisiin direktiiviviittauksen sijaan suoraan CSIRT-yksikölle asetettavista vaatimuksista. Yhdessä lausunnossa todettiin, että kaupallisia CSIRT-palveluita on saatavilla, ja olisi hyvä, ettei viranomainen omilla toimillaan laajenisi tälle markkinalle.

Lausunnoissa pidettiin tärkeänä, että CSIRT-yksikkö loisi toimintamalleja ja ohjeistuksia erilaisille toimijoille ja aloille kyberturvallisuuden vahvistamiseksi ja poikkeustilanteisiin vastaamiseksi. CSIRT-yksikön toivotaan myös tarjoavan asiantuntija-apua valvoville viranomaisille.

Puolustusministeriö esitti harkittavaksi, pitäisikö lainsäädännössä mahdollistaa uusien CSIRT-yksiköiden perustaminen tarvittaessa, jotta voitaisiin joustavoittaa kyberturvallisuuden toteutumista kansallisella tasolla.

Lausunnoissa tuotiin esille, että CSIRT-yksikön tehtäviä tulisi selkeyttää suhteessa sen toimivaltuuksiin. Lausunnoissa tuotiin esille, että CSIRT-yksikölle ei ole säädöstasolla osoitettu NIS2-direktiivin 10 artiklan 1 kohdassa tarkoitettua tehtävää ”poikkeamien käsittelyn vastaamisesta”. CSIRT-yksikön roolia poikkeamailmoitusten käsittelyssä toivottiinkin selkiytettävän ja tarjotun avun laatua sekä reagointiaikaa määriteltävän tarkemmin. Onnettomuustutkintakeskuksen mukaan saattaisi olla tarpeen täsmentää säädökseen, mikä olisi CSIRT-yksikön tekemän tutkinnan laajuus, sisältö ja lopputuote.

Yhteistä koordinaatiota ja tiedonvaihtoa sekä toimijoilta CSIRT-yksikölle, että CSIRT-yksiköltä toimijoille pidettiin hyvänä erityisesti useisiin toimijoihin kohdistuvien hyökkäysten torjumisessa. Lausunnoissa kannatettiin sitä, että CSIRT-yksikön tehtäviin sisällytettäisiin vielä lain tasolla NIS2-direktiivin 11 artiklan 4 kohtaan sisältyvä velvoite luoda yhteistyösuhteet asiankuuluviin yksityisen sektorin sidosryhmiin.

Useat lausunnonantajat pitivät haavoittuvuuskartoitusta koskevaa toimivaltuutta kannatettavana. Lausunnoissa pidettiin parempana, jos toimivaltuus sidottaisiin kokonaisuudessaan kohteen suostumukseen. Lausuntopalautteessa katsottiin lisäksi, että haavoittuvuuskartoitus tulisi suorittaa tunkeilemattomasti eli ei-intrusiviisella tavalla (non-intrusive) ja ennakoidusti sopien yritysten kanssa. Oikeusministeriö toi esiin haavoituskartoituksen osalta luottamuksellisen viestinnän suojaa koskevia perusoikeusnäkökulmia ja perustelutarpeita. Poliisihallitus puolestaan kiinnitti huomiota toimivaltuuden suhteesta mm. tietomurron tunnusmerkistöön. Lausunnoissa nostettiin esille myös kysymyksiä eri maiden CSIRT-yksiköiden tekemien haavoittuvuuskartoituksien koordinaatiosta.

Koordinoituun haavoittuvuuksien julkistamiseen liittyen katsottiin tarpeelliseksi selventää, liittyykö siihen ilmoitusvelvollisuus vai koskeeko säännös kenen tahansa CSIRT-yksikölle ilmoittamia haavoittuvuuksia. Puolustusministeriön mukaan CSIRT-yksiköllä tulisi olla velvollisuus ottaa mukaan toimintaan myös muita viranomaisia, kuten kyberkriisinhallintaviranomaiset. Toisaalta lausunnoissa pohdittiin myös riskejä, joita liittyy sensitiivisen datan keräämiseen yhteen paikkaan. Lausunnoissa tuotiin esiin myös sitä näkökulmaa, että tietojen siirto yhdeltä toimijalta toiselle on aina riski, ja että turhia tiedonsiirtoja tulisi välttää.

Liikenne- ja viestintäviraston mukaan ehdotetut säännökset CSIRT-yksikön luottamuksellisesta asemasta parantaisivat kyberturvallisuuteen liittyvien uhkatietojen jakamista esimerkiksi suomalaisille huoltovarmuuskriittisille organisaatioille, jotta nämä voisivat parhaalla mahdollisella tavalla suojautua kyberuhkilta ja poikkeamilta. Liikenne- ja viestintävirasto korosti tarvetta säilyttää

CSIRT-yksikön luottamuksellinen rooli suhteessa toimijoihin, joita se tukee, jotta CSIRT-yksikön toiminta tietoturvaloukkausten tutkimiseksi ja selvittämiseksi ylipäätään on mahdollista.

Sisäministeriö ja Poliisihallitus pitivät ongelmallisena esityksen 24 §:n 3 momenttiin sisältyvää säännöstä siitä, että CSIRT-yksikön saamaa muuta kuin pakollisen ilmoitusvelvollisuuden alaan sisältyvää tietoa ei saisi käyttää tiedon luovuttanutta koskevassa rikostutkinnassa eikä hallinnollisessa tai muussa tiedon luovuttanutta koskevassa rikostutkinnassa. Ehdotuksen arvioidaan rajaavan merkittävän määrän tietoa ulkopuolelle siitä, mitä voitaisiin tietoverkkorikosta tutkittaessa hyödyntää ja voivat johtaa tilanteeseen, jossa asianomistaja on eri asemassa sen mukaan, kuuluuko ilmoituksen tehnyt taho pakollisen ilmoitusvelvollisuuden piiriin, vai onko ilmoitus tehty vapaaehtoisesti. Lausunnoissa ehdotetaan, että kirjaus poistettaisiin tai sitä tarkennettaisiin vähintään törkeimpiä rikoksia koskien.

Oikeusministeriö edellytti tarkennuksia vapaaehtoisiin jakamisjärjestelyihin osallistuviin tahoihin sekä siihen liittyvään tiedonvaihto-oikeuteen liittyviin säännöksiin. Oikeusministeriö toi esiin ehdotukseen liittyviä valtiosääntöoikeudellisia näkökulmia ja totesi, että tietojen luovuttaminen vaikuttaisi muodostuvan hyvin väljän sääntelyn varaan, jota ei voida pitää perustuslain kannalta ongelmattomana siinä tapauksessa, että kyberhyökkäyksen toteuttamiseksi luodun haitallisen tietokoneohjelman tai käskyn sisältävän viestin katsottaisiin nauttivan luottamuksellisen viestin salaisuuden suojaa. Lausunnoissa pidettiin tarpeellisena tarkentaa, ketä tiedonvaihtoon voisi osallistua. Lausunnoissa pidettiin toisaalta perusteltuna, ettei tiedonvaihtoa olisi rajattu vain lain velvoitteiden soveltamisalaan kuuluvien yritysten tai julkisyhteisöjen väliseksi. Yhdessä lausunnossa katsottiin, että NIS2-direktiivin 29 artiklan mukaisen kyberturvallisuustietojen jakamisjärjestelyyn osallistuminen tulisi olla direktiivin soveltamisalaan kuuluvien toimijoiden osalta pakollista, jotta jakamisjärjestelystä olisi siihen osallistuville organisaatioille konkreettista hyötyä. Kukin toimija pystyisi järjestelyssä jaettavasta tiedosta rajaamaan pois organisaatiolleen tärkeät ja mahdolliset arkaluonteiset tiedot keskittyen uhkatekijän kannalta olennaisen tiedon jakamiseen.

Lausunnoissa toivottiin myös uudelleentarkastelua ja täsmentämistä esitysehdotuksen luottamuksellisen viestintätiedon käsittelyä koskeviin poikkeuksiin. Erityisesti esitysehdotuksen 20§ ja 22§ perusteluineen sisältävät sekä sisäisiä ristiriitoja että epäselvyyttä siitä, mikä on kunkin tahon käsittelyperuste ja kattaako se myös välitystiedon käsittelyn. FiCom ry:n lausunnossa pidettiin tärkeänä täsmentää, puhutaanko esimerkiksi (telepäätelaitteiden) yksilöintitiedoissa välitystiedosta, ja milloin CSIRT-yksiköllä tarkalleen ottaen on oikeus käsitellä välitystietoja ja milloin ei.

Oikeusministeriö totesi CSIRT-yksikön toiminnasta perittäviä maksuja koskevassa säännöksessä olevan asetuksenantovaltuuden turhaksi ja piti perustellumpana säännöstä, jossa todettaisiin, että kyseisistä palveluista voidaan periä maksu sen mukaan kuin maksuperustelaissa säädetään.

Lausunnoissa esitettiin huoli CSIRT-yksikön resurssien riittävyydestä sille tarkoitettuihin tehtäviin ja tarve varmistaa resurssien riittävyys myös jatkossa.

Kyberala ry ja eräät muut lausunnonantajat toivat esiin lausunnoissaan kysymyksiä ja haasteita liittyen muun muassa monialaisten ja –kansallisten yhtiöiden laajojen IP-osoitealueiden sekä niitä koskevien haavoittuvuustietojen huomioimiseen esityksessä.

Tiedonhallintalakia ja täytäntöönpanoa julkishallinnossa koskevat huomiot

Kyberturvallisuuden riskienhallinta- ja raportointivelvoitteiden laajenemista myös julkishallintoon pidettiin yleisellä tasolla perusteltuna lausuntopalautteessa.

Yhdessä lausunnossa katsottiin, että NIS2-direktiivin suomenkielisessä kieliversiossa julkishallinnon toimijoista käytetty termi ”keskustason julkishallinnon toimija” on käsitteenä laajempi kuin englanninkielisessä kieliversiossa käytetty ”central government”. Jatkovalmistelussa toivottiin arvioitavan, voivatko valtionhallinnosta erilliset organisaatiot olla osa valtion keskushallintoa tai kuulua direktiivin määritelmään.

Eduskunnan kanslia katsoi, että esityksessä on otettu asianmukaisesti huomioon NIS2-direktiivin velvoitteiden soveltamisalan rajaus siten, että tiedonhallintalain 4 a luvun soveltamisalan ulkopuolelle rajautuisivat tuomioistuimet, valitusasioita käsittelemään perustetut lautakunnat, Suomen pankki sekä eduskunnan valtiopäivätoiminta ja eduskunnan virastot. Oikeuskanslerinviraston lausunnon mukaan valtioneuvoston oikeuskanslerin osalta ehdotettu sääntely vastaa noudatettua sääntelytapaa (esim. tietosuojalain 14.2 §), jossa ylin laillisuusvalvoja suljetaan nimenomaisilla säännöksillä muun viranomaisvalvonnan ulkopuolelle. Lain 3 §:n säännökset jättävät eduskunnan virastot, esim. valtiontalouden tarkastusviraston sekä eduskunnan oikeusasiamiehen, kokonaan lain 4 a luvun soveltamisen ulkopuolelle. Direktiivin 6 artiklan 35 kohta ei sinällään tätä edellyttäisi, sillä direktiivissä käytetyllä käsitteellä ”parlamentti” viitataan kansanedustuslaitoksen toimintaan, Suomessa eduskunnan valtiopäivätoimintaan. Eduskunnan virastot on yleensä kansallisessa lainsäädännössä säädetty yleislakien piiriin kuuluviksi. Oikeuskanslerin viraston lausunnon mukaan jatkovalmistelussa tulisi vielä tarkistaa tiedonhallintalain 3 §:n säännökset näiltä osin.

Tuomioistuinviraston lausunnon mukaan ehdotetussa lakitekstissä ja hallituksen esityksen perusteluissa tuomioistuinten rajaaminen lain soveltamisalan ulkopuolelle on tehty hyvin epäselvästi. Tuomioistuinvirasto kuvaili, kuinka Tuomioistuinviraston tehtävänä on muun ohessa ”huolehtia tuomioistuinten tietojärjestelmien ylläpidosta ja kehittämisestä” (Tuomioistuinlain 19 a luvun 2 §:n 2 mom). Tuomioistuinvirasto vastaa siis muun muassa tuomioistuinten lainkäyttötehtävissä hyödynnettävien asianhallintajärjestelmien ylläpidosta ja kehittämisestä. Hallituksen esityksen perusteella jää epäselväksi, mikä vaikutus direktiivin mukaisella soveltamisalan rajauksella on Tuomioistuinviraston toimintaan tuomioistuinten tietojärjestelmien kehittäjänä ja ylläpitäjänä. Tuomioistuinviraston lisäksi kysymys tuomioistuimia koskevan soveltamisalan rajoituksen heijastusvaikutuksesta on merkityksellinen tuomioistuimille palveluita tuottavien Oikeusrekisterikeskuksen ja Valtion tieto- ja viestintätekniikkakeskus Valtorin kannalta.

Ulkoministeriö katsoi, että hallituksen esityksestä puuttuu NIS2-direktiivin 8. johdantokappaleen mukainen rajaus, että direktiiviä ei sovelleta julkishallinnon toimijoihin, jotka on perustettu yhdessä kolmannen maan kanssa kansainvälisen sopimuksen mukaisesti eikä jäsenvaltioiden kolmansissa maissa sijaitseviin diplomaattisiin edustustoihin ja konsuliedustustoihin tai näiden verkko- ja tietojärjestelmiin, siltä osin kuin tällaiset järjestelmät sijaitsevat edustuston tiloissa tai niitä ylläpidetään kolmannessa maassa olevia käyttäjiä varten. Ulkoministeriö pyysi lisäämään tästä soveltamisalan rajauksesta nimenomaisen säännöksen täytäntöönpanolainsäädäntöön ja asianmukaisesti perustelutekstiin.

Oikeusministeriö piti perusteltuna, että tiedonhallintalain 3 §:n 2 momenttia tarkistetaan sen osalta, että valvonnan ulkopuolelle rajattaisiin myös eduskunnan oikeusasiamies.

Sosiaali- ja terveysministeriö kannatti ehdotusta siitä, että Kela kuuluisi sääntelyn soveltamisalaan. Esityksen mukaan valvovan viranomaisen valvontatoimivaltuuksia ja tiedonsaanti- sekä tarkastusoikeutta ei kuitenkaan perustuslaillisista syistä sovellettaisi tasavallan presidentin kansliaan, valtioneuvoston oikeuskanslerin toimintaan eikä Kansaneläkelaitokseen. NIS2-valvonta voitaisiin kuitenkin toteuttaa eduskunnan nimeämien valtuutettujen kautta, heidän suorittaman normaalin valvonnan osana, esimerkiksi vuosiraportoinnilla. Kela katsoi, että tiedonhallintalain 18 §:n tulisi koskea myös Kelaa.

Sisäministeriön pelastusosasto ja Hätäkeskuslaitos katsovat, että myös Hätäkeskuslaitos tulee rajata tiedonhallintalain 4 a luvun soveltamisalan ulkopuolelle. Lisäksi esitystä tulisi tarkentaa siltä osin, kuuluuko Pelastusopisto tiedonhallintalain soveltamisalaan vai ei. Pelastusopisto on toisaalta tiedonhallintalain tarkoittama itsenäinen julkisoikeudellinen laitos, johon pääsääntöisesti on sovellettava direktiiviä, mutta toisaalta myös kansallisen liikkumavaran alaan kuuluva opetus- ja koulutusalan laitos. Sisäministeriön näkemyksen mukaan Pelastusopisto voitaisiin rajata tiedonhallintalain 4 a soveltamisalan ulkopuolelle.

Tulli totesi, että tietoturvallisuuden kokonaisuuden hallinnan kannalta tarkoituksenmukaisinta olisi käsitellä Tullia yhtenä kokonaisuutena, jossa tiedonhallintalakia sovelletaan samoilla yhtenäisillä periaatteilla koko Tulliin. Soveltamisen tulisi määräytyä yhtenevästi muiden turvallisuusviranomaisten kanssa. Tulli katsoi, että koska koko Tullin toiminta pääosin suojaa yhteiskuntaa, ympäristöä ja kansalaisia, olisi sen toiminta kokonaisuudessaan jätettävä direktiivin soveltamisalan ulkopuolelle, ei pelkästään Tullin rikostorjunta.

Eläketurvakeskuksen asemaan liittyen todettiin, että Eläketurvakeskuksesta annetun lain 1 §:n mukaan se on yksityisten alojen työeläketurvan toimeenpanon ja kehittämisen yhteiselin. Perustuslakivaliokunta on todennut, ettei Eläketurvakeskus ole viranomainen (PeVL 30/2005 vp). Sinällään Eläketurvakeskus on EU-oikeudellisesti katsottuna julkisoikeudellinen laitos. Eläketurvakeskus pitää johdonmukaisena, että tiedonhallintalain soveltamisala säilyisi yhdenmukaisena yksityisten alojen työeläkevakuuttajien kanssa eikä tiedonhallintalain 4 a lukua sovellettaisi Eläketurvakeskukseen. Eläketurvakeskus katsoi myös, että mikäli tiedonhallintalain 4 a lukua esitettäisiin sovellettavaksi Eläketurvakeskukseen, siitä tulisi säätää toisella tavalla kuin mitä luonnoksessa tällä hetkellä on tiedonhallintalain 3 §:n 2 momentissa esitetty.

Suomen itsenäisyyden juhlarahasto Sitra pyysi täsmentämään, kuuluisiko se uuden tiedonhallintalakiin esitetyn 4 a luvun soveltamisalaan ottaen huomioon, että se on eduskunnan vastattavana oleva itsenäinen julkisoikeudellinen rahasto, jonka toimintaan sovelletaan hallintolakia, kielilakia, julkisuuslakia ja sähköisestä asioinnista viranomaistoiminnassa annettua lakia.

Luonnonvarakeskus piti epäselvänä, soveltuvatko velvoitteet myös sen toimintaan.

Lausuntopalautteessa todettiin, että jatkovalmistelussa olisi syytä arvioida miltä osin Suomen Erillisverkot Oy voi luokitella itsenäisesti tuottamiaan asiakirjoja ja miltä osin luokittelun tekee toimeksi antanut viranomainen, erityisesti kun yrityksellä näyttää olevan palvelutehtäviä eri viranomaisille, jolloin se toimii niiden lukuun julkisuuslain tarkoittamalla tavalla. Tällöin myös yrityksen laatimat asiakirjat ovat toimeksi antaneen viranomaisen asiakirjoja.

Tiedonhallintalautakunnan mukaan tiedonhallintalakiin ehdotettavan uuden luvun määritelmiä tulisi yhteensovittaa tiedonhallintalain olemassa olevien käsitteiden kanssa. Yhdessä lausunnossa

huomautettiin, että on myös muita tietoturvaan liittyviä vaatimuksia (Julkri, Katakri, Pitukri, ISO-standardit ja soveltamisohjeet) eri TVT-palvelutyypeille. Näiden suhde lausunnolla olevaan esitykseen tulisi kuvata selkeämmin. Yhden lausunnonantajan mukaan on tärkeää, että tiedonhallintalautakunnan ja Liikenne- ja viestintäviraston antamat ohjeet ja suositukset eivät ole ristiriitaisia. Tiedonhallintalautakunnan ja Liikenne- ja viestintäviraston yhteistyötä tietoturvallisuuteen ja kyberturvallisuuteen liittyvien ohjeiden ja suositusten laatimisessa korostettiin.

Yhdessä lausunnossa toivottiin, että tiedonhallintalautakunta antaisi säilytysaikasuosituksia esitykseen sisältyvien ehdotusten mukaiseen dokumentaatioon liittyen.

Tasavallan presidentin kanslia toi lausunnossaan esille näkökohtia sääntelyn soveltamisesta tasavallan presidentin kansliaan. Eduskunnan kanslia ja tasavallan presidentin kanslia nostivat esille kysymyksen, onko luonnoksessa esitetyn tiedonhallintalain 18 g §:n mukaisessa tiedotusvelvollisuudessa merkittävästä kyberuhasta ja poikkeamasta joltain osin kyse sellaisesta valvonnasta, jota ei tulisi kohdistaa ylimpiin laillisuusvalvojiin - erityisesti 18 g §:n 3 momentin mukaisessa velvoittamisessa tiedottamaan merkittävästä poikkeamasta.

Yksi lausunnonantaja huomautti, että tiedonhallintalakiin ehdotettavan 18 l §:n mukaan Liikenne- ja viestintävirasto voi antaa viranomaiselle huomautuksen tai varoituksen. Säännöksestä ei kuitenkaan ilmene, mistä huomautus tai varoitus voidaan antaa.

Kahdessa lausunnossa kommentoitiin tiedonhallintalakiin ehdotettua riskin määritelmää siten, että se on liian kapea-alainen ja sidottu ehdotettuun uuteen kyberturvallisuussääntelyyn. Riskien arvioinnista on säädetty myös muualla tiedonhallintalaissa, joten käsitteen suhdetta tulisi arvioida esityksessä koko tiedonhallintalakiin. Se ei vaikuttaisi olevan ongelmitta sovitettavissa muuhun sääntelyyn kapea-alaisuutensa vuoksi.

Verkkotunnusvälittäjiä koskevat huomiot

Liikenne- ja viestintävirasto katsoo, että esitysluonnoksessa sähköisen viestinnän palveluista annetun lain 167 §:n 2 momentilla pyritään käytännössä automaattiseen ratkaisumenettelyyn riskiarvion perusteella tunnistettujen verkkotunnusten rekisteröinnin estämisen nopeuttamiseksi. Liikenne- ja viestintävirasto ehdottaa siksi sähköisen viestinnän palveluista annetun lain 43 lukuun lisättäväksi hallinnollinen oikaisuvaatimusmenettely, joka olisi välttämätön automaattisessa ratkaisumenettelyssä.

Poliisihallitus katsoo, että sähköisen viestinnän palveluista annetun lain 167 §:n muutosesityksen 2 momentista ”voi estää” tulisi muuttaa muotoon ”estää”. Poliisihallitus katsoo, että säännöksen ei tulisi olla muodossa, jossa viranomainen voisi sallia virheellisten tai puutteellisten tietojen tallentamisen viranomaisen rekisteriin. Yhdessä lausunnossa pyydettiin myös kiinnittämään huomiota siihen, että verkkotunnusvälittäjillä ja verkkotunnusten rekisteröintipalveluja tarjoavilla toimijoilla on jokin takaraja tietojen päivittämiselle, sillä joissain tilanteissa verkkotunnusvälittäjään on saatava yhteys hyvin nopeasti käynnissä olevan oikeudenloukkauksen lopettamiseksi ja tällöin yhteystietojen olisi oltava ajan tasalla.

TTVK huomautti, että NIS2-direktiivissä asetetaan verkkotunnusten rekisteröintitietojen tarkistusvelvollisuus aluetunnusrekisterin lisäksi yksiselitteisesti myös verkkotunnusten

rekisteröintipalveluja tarjoaville toimijoille, ja että ehdotettu kansallinen lainsäädäntö ei täysin vastaisi tätä.

Oikeusministeriö toteaa, että ehdotetun 167 §:n 5 momentin sekä 170 §:n määräyksenantovaltuuden sisältö vaikuttaa sellaisten luonteeltaan yleisten oikeussääntöjen antamiselta, joka tulisi sääntelyn merkityksen vuoksi toteuttaa lain tasoisella säädöksellä.

Musiikintuottajat ry:n lausunnossa katsottiin, että NIS2-direktiivi asettaa selkeän määräajan sille, missä ajassa verkkotunnusten rekisteröintitietoja koskeva tietopyyntö on käsiteltävä, eikä esitysteksti vastaa direktiivin muotoilua. Rekisteröintitietojen saatavuus ja nopea käytettävyys niihin pääsyä oikeutetusti pyytäville on olennaisen tärkeää DNS-järjestelmän väärinkäytön ehkäisemiseksi ja torjumiseksi sekä poikkeamien ehkäisemiseksi, havaitsemiseksi ja hallitsemiseksi.

Kyberturvallisuusstrategia ja laajamittaisten kyberpoikkeamien ja –kriisien hallintasuunnitelma

Sisäministeriö kannattaa laajamittaisten kyberpoikkeamien ja -kriisien hallintasuunnitelmien tekemiseen ehdotettua yhteistoimintamallia (45 §) sekä 46 §:ään sisältyvää yhteistyövelvoitetta. Puolustusministeriö esittää, että 46 §:än lisättäisiin mahdollisuus toimia yhteistyössä myös Puolustusvoimien kanssa tai vaihtoehtoisesti kyberkriisinhallintaviranomaisten kanssa.

Puolustusministeriö toteaa, että kyberkriisinhallintaviranomaisten tehtävistä sinänsä ei ole tarkempaa sääntelyä, mikä saattaa jättää kyseisten viranomaisten tehtävät ja roolit epäselviksi. Puolustusministeriö esittää, että edellä mainittua tarkennettaisiin ainakin perusteluissa.

Kumottavaksi ehdotettuja säännöksiä koskevat huomiot

Velvoitteiden keskittämistä uuteen toimialarajat ylittävään lakiin pidettiin lausunnoissa lähtökohtaisesti kannatettavana. Kumottavaksi ehdotettuja säännöksiä koskevia huomioita esitettiin lausuntopalautteessa niukasti.

FiCom ry:n lausunnossa pohditaan, onko tarpeen, että sähköisen viestinnän palveluista annetun lain 275 §:ssä on edelleen mukana teleoperaattoreiden erillisvelvoite raportoida tietoturvauhista Traficomille, vai olisiko selkeämpää, että raportointivelvoitteet olisi selkeästi koottu lakiin kyberturvallisuuden riskienhallinnasta, ja sektorikohtaisesta lakitasoisesta sääntelystä luovuttaisiin.

Energiavirasto kannattaa NIS1-direktiivin täytäntöönpanemiseksi annettujen säännösten kumoamista lainsäädännöllisten ristiriitojen välttämiseksi.

Sosiaali- ja terveysalan lupa- ja valvontavirasto Valvira ei kannata asiakastietolakiin ehdotettuja muutoksia. Valvira katsoo, että asiakastietolain 90 §:n 3 momenttiin ehdotettu teknisluonteinen ja päällekkäisyyksien välttämiseen tähtäävä viittaus kyberturvallisuuden riskienhallinnasta annettavaan lakiin tosiasiallisesti kaventaisi nykyisten palveluntuottajien ilmoitusvelvollisuuksia häiriötilanteissa siten, että ilmoitusvelvollisuus koskisi jatkossa vain suurempia terveydenhuollon palvelunantajia. Vaikka asiakastietolain 90 §:n 3 momentin mukainen ilmoitusvelvollisuus ja Valviran toimivalta tiedottaa itse merkittävistä poikkeamista vastaisi sisällöllisesti ehdotetun kyberturvallisuuden riskienhallinnasta annetun lain 14 §:n 3 momentin mukaista ilmoitusta, koskisi

jälkimmäinen säännös vain osaa asiakastietolain mukaisia palvelunantajia. Valvira ehdottaa, että asiakastietolain 90 §:n 3 momenttia ei muutettaisi NIS2-toimeenpanossa ehdotetulla tavalla.

Kaksi lausunnonantajaa huomautti, että asiakastietolain 82 §:ssä ja 90 §:ssä on säädetty määräyksenantovaltuudesta Terveyden ja hyvinvoinnin laitokselle, ja että nämä määräystoimivaltuudet olisivat päällekkäisiä NIS-sääntelyn kanssa. Lausunnonantajat ehdottivat joko asiakastietolain muuttamista tai määräyksenantovaltuuksien suhteen selkiyttämistä.

Vaikutustenarviointia koskevat huomiot

Esityksen vaikutustenarviointia pidettiin sinänsä kattavana, mutta lausunnoissa tuotiin esiin tarve pyrkiä edelleen tarkempaan vaikutustenarviointiin. Lausunnoissa esitettiin joitakin yksityiskohtaisempia huomioita vaikutusarvioinneista sekä yleisemmin näkemyksiä kyberturvallisuuteen sekä viestintäverkkoihin ja tietojärjestelmiin liittyvistä vaikutusarvioinneista.

Valtiovarainministeriö huomauttaa, että julkisen sektorin henkilöresurssitarpeita arvioidessa tulisi ensisijaisesti pyrkiä priorisoimaan tehtäviä ja kuluja hallinnonalan sisällä. Valtiovarainministeriö pyytää lisäksi kiinnittämään huomiota siihen, että julkisen talouden tilanne on edelleen heikko ja että kansallisesta resursoinnista päätetään talousarviossa ja julkisen talouden suunnitelmassa. Mikäli esityksestä aiheutuisi muutoksia viranomaisten toimintamenoihin, tulisi esitys antaa eduskunnalle budjettilakina ja se tulisi käsitellä raha-asiainvaliokunnassa.

Lausunnoissa todettiin, että monet esitetyistä muutoksista edellyttävät hallinnonalojen palvelukeskuksilta uusia kyvykkyyksiä, kuten esimerkiksi tiedonhallintayksikkökohtaisia räätälöityjä selvityksiä sekä valvontatoimia. Näitä uusia kustannuksia ei välttämättä pystytä kattamaan valtion talousarvion mukaisista määrärahoista ilman lisärahoitusta. Lausuntopalautteessa esitettiin myös joitakin arvioita sääntelyn noudattamisesta aiheutuvista kustannuksista kyseisen lausunnonantajan osalta. Lausunnoissa katsottiin, että vaikutustenarviointia tulisi täydentää sen osalta, millaisia vaikutuksia sääntelyn noudattamisesta aiheutuu julkishallinnon toimijoille. Yksi lausunnonantaja katsoi, että esityksessä on asianmukaisesti arvioitu tiedonhallintalain soveltamisalaan kuuluvalle toimijalle ehdotuksesta aiheutuvat lisäresurssitarpeet. Turvallisuus- ja kemikaaliviraston mukaan julkisen hallinnon edellytyksiä suoriutua uusista tehtävistä voitaisiin parantaa ja tehostaa esimerkiksi yhteisillä asiantuntijaresursseilla sekä järjestämällä säädöksen toimeenpanoa tukevaa koulutusta koordinoidusti julkisten organisaatioiden johdolle ja asiantuntijoille. Hallituksen esitystä olisi suositeltavaa täydentää yhteisten resurssien ja osaamisen koordinoinnin näkökulmasta. Energiavirasto arvioi tarvitsevansa erillisen asiankäsittelyjärjestelmän lain täytäntöönpanon myötä, ja arvioi, että olisi tarkoituksenmukaista ja kustannustehokasta rakentaa viranomaisten yhteinen sähköinen järjestelmä, johon valvovat viranomaiset saavat käyttöoikeudet ja, jossa voi käsitellä TL III-luokiteltua materiaalia.

Esityksessä esitettyihin lisäresurssitarpeisiin esitettiin joitakin tarkennuksia muun muassa Etelä-Savon ELY-keskuksen, Fimean, Valviran ja Tukesin osalta. Useissa lausunnoissa toivottiin, että esitysluonnoksessa kiinnitetään erityistä huomiota riittävien resurssien turvaamiseen Traficomille myös tämän esityksen piirissä olevien tehtävien ulkopuolella. NIS2-direktiivin toimeenpano ei saisi heikentää Traficomin ja Kyberturvallisuuskeskuksen muuta perustyötä. Myös toimijoihin kohdistuvien vaikutusten osalta esitettiin useita sektorikohtaisia tarkennuksia ja täsmennystarpeita.

Tiedonhallintalautakunta katsoi, että ehdotuksen johdosta sen on tehtävä muutoksia toiminnan suunnittelun ja suositusten valmistelun menettelyihin sekä viestintä- ja neuvontakäytäntöihin. Muutosten vaatiman työn arvioidaan kuitenkin olevan määräaikaista ja suhteellisen vähäistä. Tämän vuoksi tiedonhallintalautakunta ei arvioi ehdotuksen edellyttävän muutoksia sen nykyiseen resurssi- ja määrärahamitoitukseen.

Oikeusministeriön mukaan esitysluonnoksessa on asianmukaisesti huomioitu tietosuojavaltuutetulle seuraavat lisätyövaikutukset. Oikeusministeriö kiinnitti kuitenkin huomiota siihen, että hallituksen esityksestä seuraisi vaikutuksia myös Oikeusrekisterikeskukselle ja hallintotuomioistuimille.

Valtiovarainministeriö kiinnitti huomiota siihen, että esityksessä ei ole erityisesti arvioitu vaikutuksia kuntiin, kuntien tehtäviin tai kustannuksiin. Valtiovarainministeriö toteaa, että esityksen vaikutukset tulisi arvioida kuntakonsernin näkökulmasta, jolloin tulisi arvoiduksi, onko sääntelyllä vaikutusta kuntatalouteen ja julkiseen talouteen. Mikäli sääntelyllä arvioidaan olevan merkittäviä vaikutuksia kuntien talouteen tai toimintaan tulisi hallituksen esitys käsitellä kuntalain (410/2015) 13 § mukaisesti neuvottelumenettelyssä Kuntatalouden ja -hallinnon neuvottelukunnassa.

Muun muassa Elinkeinoelämän keskusliitto piti hyvänä, että valmistelussa on tilattu selvitys taloudellisten vaikutusten arvioinnista. Elinkeinoelämän keskusliitto kuitenkin katsoo, että vaikutuksia tulisi arvioida vielä yksityiskohtaisemmin ja sitä tulisi laajentaa myös muille toimialoille. Lisäksi lausunnossa huomioitiin, että valvovat viranomaiset voisivat antaa sellaisia sektorikohtaisia määräyksiä, joiden toteuttaminen voisi olla kallista.

Osa lausunnonantajista piti vaikutustenarviointia puutteellisena. Yksi lausunnonantaja esitti, että arvio IT-kustannuksien 12–22 % kasvusta, riippuen organisaation kyberturvallisuuden hallintamallin lähtötasosta, voi tuoda yllättäviä lisäkustannuksia, joihin ei ole varauduttu pidemmällä aikavälillä. Yhdessä lausunnossa arvioitiin, että hallituksen esityksen taloudelliset vaikutukset säädöksen määräyksiä toteuttaville toimijoille on arvioitu ylioptimistisesti.

Yksi lausunnonantaja arvioi, että erityisesti kustannuksia tulee aiheutumaan poikkeamahavainnoinnin ja poikkeamaraportoinnin järjestämisestä säädetyissä aikarajoissa sekä sellaiset järjestelmät, joiden elinkaari on suunniteltu pitkäksi ja joiden uusimisesta aiheutuisi merkittäviä kustannuksia.

Sääntelyn lisääntyminen yleisesti nähtiin lausunnoissa haasteena yrityksille. Toimintaa digitaalisessa ympäristössä koskeva sääntely on lisääntynyt ja lisääntymässä. Sääntelyn yhteisvaikutuksesta ei ole tarpeeksi kattavaa kokonaiskuvaa. Lausunnoissa katsottiin, että esityksessä tulisi käsitellä tarkemmin yhtiövaikutuksia suhteessa monikansalliseen yritykseen sekä konsernirakenteessa (emo- ja tytäryhtiö) toimiviin yrityksiin.

Kolme lausunnonantajaa piti tarpeellisena, että täytäntöönpanosta aiheutuvien kustannusvaikutusten alentamiseksi tarjolla olisi yhtenäisiä toimintamalleja, dokumenttipohjia, koulutuksia, työkaluja, ohjeistuksia ym. täytäntöönpanon tueksi. Erityisesti CSIRT-yksikön toivottiin toimivan käytännön soveltamisen ja ohjeistamisen koordinoijana. Ohjeiden, suositusten yms. valmistelun tueksi ehdotettiin järjestettävän toimialakohtaisia keskusteluja arvoketjun yritysten ja ohjeistavien tai valvovien viranomaisten kesken.

Yksi lausunnonantaja katsoi, että kyberturvallisuustason parantamisella on myös positiivisia liiketaloudellisia vaikutuksia yrityksille. Oikeusministeriö katsoi, että ehdotetulla sääntelyllä olisi myönteisiä vaikutuksia tietoturvallisuuden kohentumisen myötä myös henkilötietojen suojaan. Tietosuojavaikutuksia toivottiin avattavan vielä enemmän. Huoltovarmuuskeskus totesi, että kyberturvallisuudella on yhteiskunnan digitalisaation myötä kasvava merkitys kansalliselle huoltovarmuudelle, ja että sääntelyn vaikutuksia huoltovarmuudelle ei ole huomioitu. Ehdotetun sääntelyn katsottiin tukevan osaltaan Suomen huoltovarmuusjärjestelmää ja sen kasvattavan sen häiriönsietokykyä.

Yhdessä lausunnossa tuotiin esille, että julkisen talouden ja erityisesti valtiontalouden sopeuttamistoimia tarkasteltaessa, tulisi jatkovalmistelussa arvioida, miten viranomaistoimintaan kohdistuvat ohjaus- ja valvontatehtävät voidaan toteuttaa tehokkaasti ministeriöiden hallinnonalat ylittäen. Tulisi arvioida, millä perusteella esimerkiksi valtiovarainministeriön hallinnonalalle on tarpeellista sisällyttää kyberturvallisuuteen ja tietoturvallisuuteen liittyviä valtionhallinnon ohjaus- ja kehittämistoimintoja, koska merkitykselliset toiminnot ovat kohdistumassa Liikenne- ja viestintävirastoon sekä tietosuojavaltuutetulle. Nyt ehdotus näyttäytyy johtavan lisämenoihin pelkästään hallinnonalarajojen muodollisuuden säilyttämiseksi. Lisäksi tulisi arvioida, missä määrin niukkoja asiantuntijaresursseja on valtionhallinnossa tarpeen ja taloudellisesti tarkoituksenmukaista hajauttaa keskitettyjen tietoturva- ja kyberturvatehtävien osalta useaan rinnakkaiseen tai päällekkäiseen toimintoon.

Muut huomiot ja avoin palaute

Lausunnoissa tuotiin laajalti esiin, että esityksen toimeenpano tuo kyberturvallisuuteen liittyviä velvoitteita uusille toimialoille ja laajentaa aiemmin soveltamisalassa olleiden organisaatioiden velvoitteita. Täytäntöönpanon tueksi katsottiin useissa lausunnoissa tarvittavan laajaa resursointia kyberturvallisuusosaamiseen ja uusien asiantuntijoiden koulutukseen. Viranomaisilta toivotaan rahoituksen kanavointia mm. kyberturvallisuuskoulutuksien järjestämiseen. Lausunnoissa tuotiin esiin erityisesti kyberturvallisuuden asiantuntijapula ja sen asettamat haasteet sääntelyn toimeenpanolle.

Toimijaluetteloon ilmoittautumista koskevaa siirtymäaikaa kannatettiin, ja lausunnoissa toivottiinkin siirtymäaikaa myös muiden velvoitteiden osalta. Joustavuutta alkuvaiheen valvonnassa ei pidetä riittävänä. Lisäksi siirtymäaikaa tarvittaisiin CER-kriittiseksi lain soveltamisen alkamisen jälkeen määritettäville yrityksille sekä mahdollisesti 3 §:n 3 momentin nojalla lain soveltamisalaan asetuksella säädettäville yrityksille.

Lausunnoissa on kannatettu hallituksen esityksen luonnoksessa esitettyä muutosta aiempaan, jonka mukaan toimijoiden velvollisuutena olisi itse tunnistaa, kuuluvatko he sääntelyn soveltamisalaan, sekä ilmoittautua valvovalle viranomaiselle toimijaluetteloon. Elinkeinoelämän keskusliitto kuitenkin katsoo, että soveltamisalan epävarmuudesta ja tulkinnallisuudesta johtuen ehdotettu toimijaluetteloon ilmoittautuminen ei ole soveltamisalaan mahdollisesti kuuluvien yritysten oikeusturvan kannalta riittävä. Lausunnoissa on ehdotettu, että viranomaisella tulisi olla velvollisuus olla etukäteen yhteydessä soveltamisalaan kuuluviin yrityksiin ja ohjeistaa oikein toimimiseksi samaan tapaan, mitä CER-direktiivissä on viranomaisen tehtäväksi asetettu. Velvollisuus ilmoittaa valvovalle viranomaiselle kahden viikon kuluessa toimijaluettelon tietojen muutoksista on koettu kohtuuttomana. Lausuntopalautteessa onkin ehdotettu, että mahdollisuuksien mukaan olisi varmistettava kyseisten tietojen siirtyminen automaattisesti eri järjestelmistä toimijaluetteloon.

Liikenne- ja viestintävirasto Traficom on kommentoinut toimijarekisterin julkisuuteen liittyviä seikkoja.

Lausunnoissa on kritisoitu IP-osoitealueiden ilmoittamisvelvoitetta. Perinteiset IP-osoitealueet, jotka on myönnetty toimijan omalle kiinteälle verkolle, koettiin helpoksi ilmaista. Sen sijaan IP-osoitteiden ilmoittaminen tuottaisi hankaluuksia organisaatioille, jotka käyttävät pilvipalveluja palvelujensa tuottamiseen. Osoitteet voivat muuttua useammin kuin omien kiinteiden verkkojen osoitteet, joten ilmoituskäytännön tulisi olla yksinkertainen, mieluiten automatisoitu rajapinta. Ilman kyseistä mekanismia, lakia ei tulisi tulkita koskemaan pilvipalvelutekniikoin tuotettavia palveluja.

Lausunnoissa tuotiin esiin, että NIS2-direktiivin ja CER-direktiivin valmistelu ja täytäntöönpano tapahtuvat osin samanaikaisesti. Esitysten välillä toivottiin hyvin toimivaa koordinaatiota, jotta yhteiskunnan kriittisimpien toimijoiden kannalta saadaan luotua toimiva sääntelykokonaisuus. Lisäksi lausunnoissa pidettiin yleisesti tärkeänä kiinnittää huomiota ehdotettavan sääntelyn yhteensopivuuteen sektorikohtaisen erityissääntelyn kanssa, jota tunnistettiin ouseilla sektoreilla.

Lausunnoissa toivottiin esitysten terminologian osalta yhdenmukaistamista asiakastietolain, kokonaisturvallisuuden sanaston ja kansainväliseen standardisointiin liittyvän terminologian kanssa. Lisäksi osa termeistä, kuten kyberhygieniakäytännöt, koettiin yleiskielelle vieraana.

Työ- ja elinkeinoministeriö toi lausunnossaan esiin, että esityksessä tulisi kiinnittää huomiota myös siihen, voivatko riskienhallintavelvoitteet muodostua elinkeinovapautta rajoittaviksi tekijöiksi, ja tarkastella siten esitystä myös elinkeinovapauden kannalta. Oikeusministeriö yhtyi esitysluonnoksessa olevaan toteamaan siitä, että haitallisen tietokoneohjelman tai käskyn sisältävän viestin käsittelyä koskevan ehdotuksen johdosta esityksestä olisi tarpeen pyytää perustuslakivaliokunnan lausunto. Oikeusministeriön näkemyksen mukaan esitys sisältää kuitenkin myös muita sen laatuisia valtiosääntöoikeudellisia kysymyksiä, joiden perusteella esitys olisi perusteltua saattaa perustuslakivaliokunnan arvioitavaksi, minkä vuoksi mainitun kirjauksen olisi syytä olla laajempi.

Ympäristöministeriö pitää tärkeänä, että esityksen jatkovalmistelussa selvitetään sitä, että onko esitystä mahdollista antaa lisätalousarvioiden yhteydessä.

Oikeusministeriö totesi, että yleisesti ottaen esitysluonnoksen lakiehdotuksissa on varsin monta säännöstä, joissa viitataan direktiivin säännökseen. Oikeusministeriö korostaa, että lähtökohtana tulee olla, että direktiiviä ei panna täytäntöön viittaustekniikalla.

Lausunnoissa tuotiin esiin erilaisia tulkintoja 1. lakiehdotuksen 4 §:n 5 momentista, joka koskisi perustetta kieltäytyä sellaisen tiedon antamisesta, jonka luovuttaminen vaarantaisi tai olisi vastoin maanpuolustuksen tai kansallista turvallisuutta koskevaa tärkeää etua. Lausuntopalautteessa korostettiin 4 §:n merkitystä myös yritysten näkökulmasta, ja todettiin että myös yrityksillä tulisi olla mahdollisuus vedota säännökseen.

Poliisihallitus katsoi lausunnossaan, ettei esityksessä ole huomioitu poliisin tarpeita tiedonsaannille kyberturvallisuuden kannalta merkittävistä uhista. Poliisihallitus korostaa, että poliisi saa tiedonhankinnan ja rikosten esitutkinnan kautta tietoa kyberturvallisuuden kannalta merkittävistä uhista, mutta esityksessä ei ole huomioitu poliisin roolia vakavien kyberrikosten estämisessä ja selvittämisessä.

Onnettomuustutkintakeskus esitti lausunnossaan harkittavaksi, olisiko säädösehdotuksiin syytä lisätä vakavista tapauksista ilmoitusvelvollisuus myös Onnettomuustutkintakeskukselle ja kirjata Onnettomuustutkintakeskuksen tutkintavelvoite näkyviin hallituksen esitykseen. Onnettomuustutkintakeskus viittaa muun ohella tarpeeseen saada vakavista tilanteista laajasti tietoa muun muassa siksi, että jokainen toimija voi osaltaan parantaa varautumistaan ja vastaavanlaisia tapauksia voitaisiin jatkossa estää. Onnettomuustutkintakeskus viittasi myös sen tehtävistä turvallisuustutkintalaissa säädettyyn sekä Petteri Orpon hallitusohjelman kirjaukseen siitä, että ”Selvitetään mahdollisuus lisätä Onnettomuustutkintakeskuksen toimialaan kyberturvallisuuteen kohdistuneiden vakavien häiriöiden turvallisuustutkinta. Hallitus valmistelee tarvittaessa säädösmuutokset turvallisuustutkintalakiin ja tekee siihen muut tarvittavat tarkistukset.”

Turvallisuus- ja kemikaalivirasto esittää lakiesitystä täydennettäväksi siten, että nimettäisiin yksi viranomainen yhtenäistämään ja koordinoimaan eri viranomaisissa tehtävää valvontaa.

Sosiaali- ja terveysministeriö pitää tärkeänä, että myös normaaliolojen häiriötilanteissa viranomaisilla on riittävästi keinoja tarvittaessa sitovasti ohjata ja johtaa tilannetta sekä mukauttaa toimintaa riittävien palvelujen ja toimeentulojen turvaamiseksi kansallisessa kokonaisturvallisuusmallissa.

Lausunnoissa pidettiin tärkeänä, että vaalikauden vaihtuessa rauenneen HE 243/2022 vp:n eli ns. KyberPTR-säädöshankkeen tavoitteita edistetään vaikuttavalla tavalla säädösvalmistelussa ja että rauenneita esityksiä voitaisiin esittää uudestaan.

Tuomioistuinviraston lausunnossa esitettiin huoli siitä, että sääntelyn kohteena oleva lainsäädäntökehikko on poikkeuksellisen monimutkainen, kun huomioidaan nyt annettavan lain ohella sähköisen viestinnän palveluista annetun lain, tiedonhallintalain sekä tietosuojasääntelyn mukaiset vaatimukset. Riskinä tällaisessa sääntelyssä on, että päällekkäiset vaatimukset johtavat ristiriitatilanteisiin lakien kesken. Lainsäädännön vaikeaselkoisuus aiheuttaa myös merkittävää hallinnollista taakkaa sitä soveltaville organisaatioille.

Erityisiä toimialakohtaisia huomioita

VR-Yhtymä esittää, että NIS2-direktiivin soveltamisala koskisi kaikkia raideliikenneoperaattoreita, sekä kaikkia rataa kunnossapitäviä toimijoita. Kyberturvallisuuden vaatimusten tulisi olla samat kaikille raideliikenteen sektorilla toimiville, riippumatta toimijoiden kokoluokasta tai toiminnan laajuudesta. VR perustelee näkemystään sillä, että Suomen rataverkko on pääasiassa yksiraiteinen ja kyberhyökkäys pienempää toimijaa kohtaan voi hankaloittaa koko junaverkon huoltovarmuutta ja aiheuttaa vakavia häiriöitä liikenteelle. VR katsoi lausunnossaan, että Suomen raideliikenne digitalisoituu ja verkottuu nopeaa tahtia, mikä nostaa kyberturvallisuusuhkia raideliikenteessä merkittävästi.

Fintrafficilla ei ole tarkkaa käsitystä siitä, katsotaanko liikenteenohjaus- ja hallintapalvelun tarjoajana toimivat julkiset ja yksityiset yritykset sellaisiksi julkishallinnon toimialan kriittisiksi toimijoiksi, joihin tullaan soveltamaan tiedonhallintalain 4 a luvun vaatimuksia vai kuuluvatko liikenteenohjaus- ja hallintapalvelun tarjoajat kyberturvallisuuden riskienhallinnasta annetun lain soveltamisalaan. Soveltamisala määrittynee lopullisesti vasta CER-lain määritelmien täsmentyessä.

Fintrafficin näkemyksen mukaan ilmailun osalta noudatettavaa EU erityislainsäädäntöä voidaan pitää NIS2-direktiivin 4 artiklassa tarkoitettuina alakohtaisena unionin lainsäädäntönä, joten NIS2 direktiivin vaatimuksia ei tulisi ulottaa koskemaan ilmailun toimijoita. Fintraffic ei pidä myöskään perusteltuna, että ilmailun toimijakentässä juuri lennonjohtopalvelun tarjoajat asetettaisiin kaksoissääntelyn alaiseksi.

Suomen Satamat ry huomioi erityisesti direktiivin soveltamisalan määrittelyyn liittyviä huomioita. Suomen Satamat ry piti satamanpitäjän määritelmiä toimivina ja tunnistettavina, mutta epäselväksi jäi, miten tunnistetaan toimijat, jotka huolehtivat rakenteista ja varusteista sataman alueella.

Posti Group Oyj ja Keskuskauppakamari pitivät valitettavana, että soveltamisalan määrittely on jäänyt tulkinnanvaraiseksi erityisesti posti- ja kuriiritoiminnan osalta.

Suomen Sähkönkäyttäjät ry piti kyberturvallisuutta erittäin tärkeänä sähkömarkkinoilla ja sähkön käyttöön liittyvissä asioissa ja arvostaa erityisesti sitä, että suljetun jakeluverkon erityisasema normaaliin jakeluverkkoon säilyy muuttumattomana.

Energiavirasto toi ilmi kokokriteeriin liittyviä huomioita, eikä pitänyt tarkoituksenmukaisena, että pienimuotoinenkin sähkön tuotanto voisi johtaa siihen, että yhtiö tulee sääntelyn soveltamisalaan ja Energiaviraston valvontaan.

Energiavirasto tuo esiin pohdinnan siitä, että jääkö edellä mainitun määritelmän myötä lain soveltamisalan ulkopuolelle merkittäviä kaukolämmityksen ja -jäähdytyksen toimijoita ja, miten valvonta järjestetään muun muassa niiden toimijoiden osalta, jotka tuottavat niin sähköä kuin lämpöä eli niin sanotut CHP-laitokset.

Yksi lausunnonantaja esitti, että elintarvikkeiden tuotanto, jalostus ja jakelu tulisi määritellä esityksessä tarkkarajaisemmin ja että lain soveltamisalasta tulisi rajata pois sellaiset keskisuuret tai isot yritykset, joiden mahdollisesti kohtaamien kyberturvallisuusriskien yhteiskunnalliset vaikutukset jäävät marginaalisiksi. Lausunnonantajan mukaan tällaisia yrityksiä olisivat esim. toimijat, joiden osalta teollinen elintarviketuotanto ja tukkukauppa kohdistuvat lähinnä oman liiketoiminnan piiriin kuuluviin yrityksiin. Samoin elintarvikkeita jakelevien yritysten osalta soveltamisalaan tulisi kuulua esimerkiksi vain sellaiset yritykset, joiden toiminta kattaa yli 0,5 % kansallisesta ruoantuotannosta. Tältä osin NIS2-direktiivi ei jätä kansallista liikkumavaraa soveltamisalan tai siihen kuuluvien määrittelemiselle. Elintarviketeollisuusliitto ry esitti vastaavan huomion siitä, että yleisen kokokriteerin soveltaminen tuo NIS2-velvoitteiden alaan merkittävän määrän elintarvikealan yrityksiä, joiden toiminnalla ei ole esimerkiksi kansallisen ruoantuotannon, turvallisuuden ja huoltovarmuuden osalta merkitystä. Elintarviketeollisuusliitto ry katsoo, että koska elintarvikealaa säädellään jo laajasti, olisi tärkeää, että lisäsääntely huomioisi kokonaiskuormitusta ja tarkoituksenmukaisuutta.

Finanssiala ry piti lausunnossaan johdonmukaisena ratkaisua siitä, että kyberturvallisuuden riskienhallinnasta annettua lakia ei sovellettaisi finanssialan toimijoihin, sillä niihin sovellettaisiin DORA-asetusta ja sitä täytäntöönpanevaa sääntelyä. Finanssiala ry katsoo, että DORA-asetus on NIS2-direktiiviin nähden erityislaki ja asettaa finanssialan toimijoille pidemmälle meneviä velvoitteita kyberuhkiin varautumiseksi.

Useat lausunnonantajat katsoivat soveltamisalan olevan haasteellinen hyvinvointialueiden kannalta. Hyvinvointialueiden vastuulle on 1.1.2023 siirtynyt sosiaalihuollon, terveydenhuollon ja

pelastustoimen palveluiden järjestäminen. Hyvinvointialueilla terveydenhuollon toimijat (sairaanhoitopiirit) ovat jo aiemmin olleet NIS1-direktiivin piirissä, mutta jatkossa hyvinvointialueet kuuluisivat NIS2-direktiivin alaan myös julkishallinnon toimialan sekä osin lääkinnällisten laitteiden valmistuksen toimialan kautta. Esityksestä ei saa selkeää käsitystä siitä, miten kyseisten viranomaisten valvontavastuut rajataan siten, ettei synny päällekkäistä valvontaa tai vastaavasti jää valvonnan ulkopuolisia osa-alueita. Varsinkin, kun hyvinvointialueiden käytännön toiminnassa ja palveluita järjestettäessä eri toimialoja on haastava erottaa toisistaan. Sekä organisaation johto, että moni tekninen ratkaisu, kuten käyttäjähallinta, työasemapalvelut tai tietoliikenneverkkoratkaisut vaikuttavat kaikkiin organisaation toimialoihin, on epäselvää, minkä valvovan viranomaisen vastuulle kuuluu näiden yhteisten osa-alueiden hallintatoimien osalta valvontavastuu. Toisaalta yksi lausunnonantaja katsoi, että hyvinvointialueen näkökulmasta soveltamisala vaikuttaa selvältä, mutta valvontaa hyvinvointialueelle suorittaa useampi viranomainen, mikä on omiaan aiheuttamaan päällekkäisyyttä.

Sosiaali- ja terveysalan lupa- ja valvontavirasto Valvira huomautti, että 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 jatkossa liittyä enenevässä määrin tilanteisiin, joissa on kyse rajat ylittävästä terveydenhuollon palvelutoiminnasta. Valvira ehdottaa sääntelyä täsmennettäväksi rajat ylittävien häiriö- ja valvontatilanteiden sekä rajat ylittävää valvontaa koskevan toimivaltasäännöksen osalta.

Sosiaali- ja terveysalan lupa- ja valvontavirasto Valvira ehdottaa kyberturvallisuuslakia täsmennettäväksi terveydenhuollon tarjoajan kansallisen määrittelyn osalta. Myös Fimea katsoo, että terveystoimialan soveltamisala vaatii kokonaisuudessaan tarkentamista, jotta lakia olisi mahdollista soveltaa ja soveltamista valvoa terveyssektorilla tarkoitetulla tavalla ja tarkoitetussa laajuudessa. Fimea katsoo, että ilman tarkentamista se ei pysty hahmottamaan omien velvoitteidensa laajuutta valvovana viranomaisena.

Fimea katsoo, että esimerkiksi ehdotetussa liitteessä II kohtien 9 ja 10 määritelmä kattaisi myös lääkinnällisiä laitteita yksilölliseen käyttöön valmistavat valmistajat, mikä laajentaa valvottavien toimijoiden määrän direktiivin tarkoittamaa laajemmaksi.

Suomen Apteekkariliitto katsoo lausunnossaan, että soveltamisalaan liittyvät toimijoiden määritelmät eivät ole selkeitä sen tulkinnan kannalta, kuuluvatko apteekit soveltamisalan piiriin. Suomen Apteekkariliitto katsoo, että apteekit eivät kuuluisi soveltamisalan piiriin.

Useissa lausunnoissa ehdotettiin, että NIS2-direktiivin kansallisen säädöksen soveltamisalaa laajennettaisiin koskemaan yksityistä sosiaalihuoltoa ja lisäksi kaksi lausunnonantajaa esittää, että laajennus koskisi myös apteekkitoimintoja. Yksi lausunnonantaja esittää, että sääntelyn soveltamisalaa laajennetaan koskemaan veripalveluja, terveydenhuollon laboratorioita sekä talousvettä toimittavien laitosten käyttämiä laboratorioita. Yksi lausunnonantaja ehdottaa, että myös sosiaalipalvelujen palveluntuottajille merkittävimpiä ohjelmistoja toimittavat yritykset huomioitaisiin soveltamisalassa ja riskienhallintavelvoitteiden osalta.

Yhdessä lausunnossa nostettiin esiin, että osa korkean riskin lääkinnällisistä laitteista voivat olla myös konfiguroitavia laitteita, ohjelmistoja tai etäluettavia laitteita. Tästä syystä esityksessä tulisi myös huolehtia siitä, että kyberturvallisuussäädökset eivät vaikuta potilasturvallisuuteen näiden laitteiden osalta.

Lausunnon antaneet korkeakoulut puolsivat yksimielisesti sitä, että esityksessä ei ehdoteta korkeakoulujen osalta käytettäväksi kansallista liikkumavaraa NIS2-direktiivin soveltamisesta opetus- ja koulutusalan laitoksiin siltä osin kuin asiassa on kansallista liikkumavaraa.

Tutkimusorganisaatioiden osalta lausunnoissa todettiin, että tutkimuslaitosympäristö aiheuttaa haasteita tietoturvatasolle. Tutkimushankkeissa joudutaan usein toimimaan epätavanomaisissa tiedonkäsittely-ympäristöissä, joiden luonnolliset riskit eivät ole rinnastettavissa tavanomaisiin toimistoympäristöihin. Kokeellisten ympäristöjen laitekanta ja ratkaisut eivät kaikilta osin ole samoilla tavoin todennettavissa ja riskiarviointi on haastavaa. Tutkimuksella on uusia ja poikkeuksellisia tavoitteita, käytössä on poikkeuksellisia teknologioita ja liityntäpinnat esimerkiksi yliopistoihin. Riskien vakavuuden ja vaikutusten arviointi on haastavaa. Sääntelyn soveltaminen tutkimuslaitosten osalta voi osoittautua haastavaksi ja edellyttää aktiivista keskustelua valvovan viranomaisen kanssa riskienhallinnan mitoittamisen osalta.

Yksi lausunnonantaja esitti huomion siitä, voisiko tutkimuslaitoksen määritelmän kautta mikä tahansa soveltamisalan kokokriteerin täyttävä yritys kuulua soveltamisalaan, jos yrityksessä on erillinen tutkimustiimi.

Turvallisuus- ja kemikaalivirasto esittää, että lakiesityksessä täsmennettäisiin kemikaalien määritelmää. Lakiesityksen liitteen II kohdassa 6, samoin kuin NIS2-direktiivin liitteen II kohdassa 3 viitataan ainoastaan REACH-asetuksen 3 artiklassa oleviin määritelmiin, joissa todetaan, että kemikaali on aine tai seos. Lakiesitys tarkoittaisi sitä, että riippumatta kemikaalin ominaisuuksista tai merkityksestä elinkeinoelämälle, niiden valmistusta tai jakelua harjoittava yritys kuuluisi sääntelyn piiriin, jos kokorajoitukset ylittyvät. Jos kaikki lukuisat kemikaalit lasketaan mukaan, niin on hyvin epäselvää, paljonko toimijoita tällöin tulisi sääntelyn piiriin. Lisäksi kaikki toimijat eivät todennäköisesti edes tunnistaisi valmistavansa kemikaalia.

Suomen taloushallintoliitto ry esitti huomioita liittyen eri toimijoiden rooleihin pilvipalvelujen ja datakeskuspalvelujen tarjoamisessa, ja korosti tarvetta selkeälle viranomaisohjeistukselle siitä, milloin yritys on toimialan piirissä ja milloin ei. Ohjeistus tulisi antaa esimerkiksi lakia alemman tasoisella säätelyllä. Lisäksi jokaisella yrityksellä tulisi olla mahdollisuus saada itseään koskeva viranomaistulkinta siitä, onko se toimialan osalta lainsäädännön piirissä.

Yksi lausunnonantaja ilmaisi huolensa siitä, että internet-yhdysliikennepisteiden toiminta on hyvin yksinkertaista, eikä palvelun hintoja ole mahdollista nostaa kattamaan regulaatiosta aiheutuvia kasvavia kustannuksia. Koska suomalaiset yhdysliikennepisteet eivät ole työnantajia, dokumentaatio pitäisi teettää konsultointityönä, mikä aiheuttaisi merkittäviä ja äkillisiä kustannuksia. Lausunnossa toivottiin, että työhön voisi saada esimerkiksi Huoltovarmuuskeskukselta rahoitusta.

Yksi lausunnonantaja huomautti, että määritelmässä ei oteta yksiselitteisesti kantaa, kuuluuko tietojärjestelmien ohjelmointityö hallintapalveluntarjoajan määritelmän piiriin. Suotavaa olisi, että tähän kysymykseen saadaan tarkennuksia, jotta TVT-palveluntarjoajat pystyvät paremmin arvioimaan, missä määrin heidän toimintaansa sovelletaan ehdotettua sääntelyä.

WithSecure Oyj esittää, että kansallisen liikkumavaran salliessa tietoturvapalveluntarjoajat määriteltäisiin kansallisessa laissa tarkkarajaisemmin.

Liitteet 1. Lausunnonantajat

LIITE: Lausunnonantajat:

Ahvenanmaan maakunnan hallitus

Burger-In Oy ja Hes-Pro Finland Oy

CSC – Tieteen tietotekniikan keskus Oy

Cyberismo Oy

Digi- ja väestötietovirasto

Eduskunnan kanslia

Eduskunnan oikeusasiamies

Elinkeinoelämän keskusliitto EK

Elinkeinoelämän keskusliitto EK - Listayhtiöiden neuvottelukunta

Elintarviketeollisuusliitto ry

Elisa Oyj

Eläketurvakeskus

Energiateollisuus ry

Energiavirasto

Espoon kaupunki

Etelä-Karjalan hyvinvointialue

Etelä-Pohjanmaan hyvinvointialue

Etelä-Savon ELY-keskus

Etelä-Savon hyvinvointialue

Etelä-Suomen aluehallintovirasto

Finanssiala ry

Finanssivalvonta (ei lausuttavaa)

Finavia Oyj

Fingrid Oyj

Gasgrid Finland Oy

Hallitusammattilaiset ry

Helsingin kaupunki

Helsingin seudun liikenne (HSL)

Helsingin seudun ympäristöpalvelut (HSY)

Helsingin yliopisto

Huld Oy

Huoltovarmuuskeskus

HUS-yhtymä

Hyvinvointiala HALI ry

Hyvinvointialueyhtiö Hyvil Oy

Hätäkeskuslaitos

Ilmatieteen laitos (ei lausuttavaa)

Innovaatiorahoituskeskus Business Finland Oy

Itä-Uudenmaan hyvinvointialue

Jyväskylän yliopisto (2 lausuntoa)

Kaakkois-Suomen Ammattikorkeakoulu Oy

Kainuun hyvinvointialue

Kansaneläkelaitos

KEHA-keskus

Keskuskauppakamari

Kymenlaakson hyvinvointialue

Liikenne- ja viestintävirasto Traficom

Liikenteenohjausyhtiö Fintraffic Oy

Luonnonvarakeskus

Länsi-Uudenmaan hyvinvointialue

Lääkealan turvallisuus ja kehittämiskeskus Fimea

Maa- ja metsätalousministeriö

Maahanmuuttovirasto

Maanmittauslaitos

Metropolia Ammattikorkeakoulu Oy

Metsähallitus (ei lausuttavaa)

Metsäteollisuus ry

Musiikkituottajat - IFPI Finland ry

Nordcloud Oy

Oikeuskanslerin virasto

Oikeusministeriö

Oikeusrekisterikeskus

Onnettomuustutkintakeskus

Opetus- ja kulttuuriministeriö

Pelastusopisto

Poliisihallitus

Posti Group Oyj

Puolustusministeriö

Päijät-Hämeen hyvinvointialue

Rakennusteollisuus ry

Rikosseuraamuslaitos

Ruokavirasto (ei lausuttavaa)

Sailab – MedTech Finland ry

Senaatti-kiinteistöt

Sisäministeriö

Solita Oy

Sosiaali- ja terveysalan lupa- ja valvontavirasto Valvira

Sosiaali- ja terveysministeriö

Suomen Apteekkariliitto

Suomen Erillisverkot Oy

Suomen Itsenäisyyden juhlarahasto Sitra

Suomen Kiertovoima ry

Suomen Kuntaliitto ry

Suomen Laivameklariliitto ry

Suomen Punainen Risti, Veripalvelu

Suomen Satamat ry

Suomen Sähkönkäyttäjät ry (ELFi)

Suomen Taloushallintoliitto ry

Suomen Varustamot ry

Suomen Vesihuoltolaitosyhdistys ry

Suomen Yrittäjät ry

Syyttäjälaitos

Säteilyturvakeskus

Tasa-arvovaltuutettu (ei lausuttavaa)

Tasavallan presidentin kanslia

Telia Finland Oyj

Teollisuuden Voima Oyj

Terveyden ja hyvinvoinnin laitos

Tiedusteluvalvontavaltuutettu (ei lausuttavaa)

TietoEVRY Oyj

Tietosuojavaltuutetun toimisto

Tietoliikenteen ja tietotekniikan keskusliitto, FiCom ry

Tilastokeskus

TREX Regional Exchanges Oy

Turvallisuus- ja kemikaalivirasto Tukes

Tulli

Tuomioistuinvirasto

TTVK ry

Työ- ja elinkeinoministeriö

Työeläkevakuuttajat TELA ry (ei lausuttavaa)

Työllisyysrahasto

Työterveyslaitos

Ulkoministeriö

Ulosottolaitos

Valtiokonttori

Valtion tieto- ja viestintätekniikkakeskus Valtori

Valtiovarainministeriö

Vantaan ja Keravan hyvinvointialue

Verizon

Verohallinto

VR Group

Väylävirasto (ei lausuttavaa)

WithSecure Oyj

Ympäristöministeriö

Yrityksen digitalous -hanke

Yhdistetty lausunto: Teknologiateollisuus ry, Finnish Information Security Cluster (FISC) – Kyberala ry sekä Puolustus- ja Ilmailuteollisuus (PIA) ry

Lisäksi lausunnon antoivat kaksi yksityishenkilöä.